COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY U.S. HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 24, 1984

[No. 123]

Printed for the use of the
Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE

39-741 O WASHINGTON : 1985

H701-39

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ALBERT GORE, JR., Tennessee
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
MERVYN M. DYMALLY, California
PAUL SIMON, Illinois
NORMAN Y. MINETA, California
RICHARD J. DURBIN, Illinois
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia
LARRY WINN, JR., Kansas
MANUEL LUJAN, JR., New Mexico
ROBERT S. WALKER, Pennsylvania
WILLIAM CARNEY, New York
F. JAMES SENSENBRENNER, JR., Wisconsin
JUDD GREGG, New Hampshire
RAYMOND J. McGRATH, New York
JOE SKEEN, New Mexico
CLAUDINE SCHNEIDER, Rhode Island
BILL LOWERY, California
ROD CHANDLER, Washington
HERBERT H. BATEMAN, Virginia
SHERWOOD L. BOEHLERT, New York
ALFRED A. (AL) McCANDLESS, California
TOM LEWIS, Florida

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
REGINA A. DAVIS, *Chief Clerk*
DAVID S. JEFFERY, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

DAN GLICKMAN, Kansas, *Chairman*

ALBERT GORE, JR., Tennessee
MERVYN M. DYMALLY, California
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MICHAEL A. ANDREWS, Texas
WILLIAM CARNEY, New York
SHERWOOD L. BOEHLERT, New York
ALFRED A. (AL) McCANDLESS, California

CONTENTS

WITNESSES

September 24, 1984:	Page
Joseph R. Wright, Deputy Director, Office of Management and Budget, accompanied by Robert P. Bedell, Deputy Administrator, Office of Information and Regulatory Affairs	4
Bruce Campbell and Frank Carr, Emergency Mobilization Preparedness Board, Executive Office of the President	28
Richard P. Kusserow, Inspector General, Department of Health and Human Services, accompanied by John I. Molnar, Program Analyst, Office of Program Inspections	40
Robert P. Campbell, president, Advanced Information Management, Inc., Woodbridge, VA, accompanied by Bruce E. Spiro, chairman, ADP System Management, Defense Communications Agency	76
Joseph B. Tompkins, Jr., chairman, Task Force on Computer Crime, American Bar Association	104

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

MONDAY, SEPTEMBER 24, 1984

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE AND TECHNOLOGY, SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS,

Washington, DC.

The subcommittee met, pursuant to call, at 1:30 p.m., in room 2318, Rayburn House Office Building, Hon. Dan Glickman (chairman of the subcommittee) presiding.

Mr. GLICKMAN. Why don't we go ahead and begin? We may have some other members coming fairly soon, but we'll start, because I know some of the witnesses have to leave.

Today the subcommittee will revisit the subject that we covered about a year ago in a series of indepth hearings: computer and communications security and privacy. What we found at that time was extremely distressing.

Computers and the communications links that connect them have become a vital tool of virtually every institution in our society. As a Nation, we have become totally dependent on them.

Yet despite their critical importance and the almost priceless value of much of the data stored within them, we have effectively ignored the threat posed by improper use or unauthorized penetration.

This situation, I regret to say, is especially severe in Government. The data in Government computers is susceptible to manipulation, penetration, and unauthorized access; and, what's worse, no one seems to be in charge. The administration's approach is basically to ignore the problem.

I'm convinced there could be several potential disasters out there just waiting to happen. A disgruntled employee, a terrorist group, or someone with criminal intent could easily disrupt or even cause irretrievable damage to our Nation. Adequate controls simply aren't in place and aren't being used.

In our hearings today, we plan to update the record, to see, as a result of our hearings last year, what actions have been taken. We've invited five witnesses from both the Government and the private sector who have been active during the past year in attempting to deal with what I feel is a problem of national dimension and consequence.

I might say that this morning I spoke at a conference held at the National Bureau of Standards, actually cosponsored by the Department of Defense and the National Bureau of Standards, on this

subject, computer security, and at that conference there were about 800 people from both the agencies, the private sector, and foreigners—a lot of foreigners were there—and several people commented to me that the national and international interest in adopting computer security, training devices, training standards, protections, to meet the incredible increase in sophisticated technology on the other side—which is the information systems, the computer enhancement, the software changes—is great indeed.

That is, not only must we move quickly on the information systems side of the picture, new and better ways to store, and to make information available to us, but we must move just as quickly to protect that information, or else all the advances of technology will be almost useless.

So today we begin by hearing from the Office of Management and Budget. We have Joseph Wright, deputy director, who was with us last year when we held testimony on this.

Mr. Wright, it's a pleasure to have you here.

I would say to all the witnesses that your entire statement will appear in the record, so you will—may feel free to summarize, if that is useful for you.

There will be a statement by Mr. Carney which will appear immediately after mine as well.

[The prepared statement of Mr. Carney follows:]

OPENING STATEMENT

HON. WILLIAM CARNEY

HEARING ON COMPUTER AND COMMUNICATIONS

SECURITY AND PRIVACY
SEPT. 24, 1984

THANK YOU MR. CHAIRMAN.

THE GRAVITY OF THE ISSUES FACING US IN TODAY'S HEARING CAN NOT BE OVERSTATED. THE HEARINGS WHICH THIS SUBCOMMITTEE HELD LAST FALL HELPED FOCUS THE PUBLIC'S ATTENTION ON THE PROBLEMS OF COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY, AND CERTAINLY THERE IS MORE AWARENESS TODAY OF THE POTENTIAL ABUSES. UNFORTUNATELY, EFFECTIVE SOLUTIONS TO THESE PROBLEMS CONTINUE TO ELUDE US, AND OUR DEPENDENCE ON AUTOMATIC INFORMATION SYSTEMS CONTINUES TO GROW.

WE CONTINUE TO READ OF COMPUTER BREAK-INS, AND PARTICULARLY ALARMING IS LEARNING THAT MOST OF THE COMPUTER CRIMES THAT ARE BEING DISCOVERED ARE BEING DSCOVERED ACCIDENTALLY. THIS CERTAINLY LEADS ONE TO SUSPECT THAT A GREAT MANY MORE SUCH CRIMES ARE BEING COMMITTED THAT GO UNDETECTED.

BUT, OF EVEN GREATER CONCERN TO ME IS THE VULNERABILITY OF OUR NATIONAL TELECOMMUNICATIONS SYSTEMS. HOW SAFE ARE THESE FROM ATTACK? DOES ANYONE EVEN KNOW?

THIS SUBCOMMITTEE, AFTER HOLDING A SERIES OF HEARINGS LAST FALL, MADE A NUMBER OF RECOMMENDATIONS, INCLUDING THE SUGGESTION THAT A NATIONAL COMMISSION BE ESTABLISHED TO EXAMINE ALL THE COMPLEX ISSUES INVOLVING COMPUTERS AND COMMUNICATION. THE WITNESSES WHO WILL BE TESTIFYING HERE TODAY SHOULD BE WELL QUALIFIED TO COMMENT ON THESE AND OTHER PROPOSALS FOR DEALING WITH THIS VERY SERIOUS PROBLEM, AND I THANK YOU AGAIN, MR. CHAIRMAN, FOR CALLING THIS HEARING.

Mr. GLICKMAN. Mr. Wright, why don't you go ahead?

STATEMENT OF JOSEPH R. WRIGHT, DEPUTY DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET, ACCOMPANIED BY ROBERT P. BEDELL, DEPUTY ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS

Mr. WRIGHT. Thank you, Mr. Chairman.

I would like, with your permission, to submit my testimony for the record and just very briefly summarize it.

You will find that in my testimony I specifically address many of the aspects of the proposed either legislation or action that the committee believes would be useful to enhance computer security, and so therefore I will not repeat my positions on each one of those items. But I would like to start by saying that, I very much appreciate and agree with many of the concerns that the committee and particularly the chairman have.

I do respectfully disagree with the lack of activity that the chairman perhaps perceives has gone on since we had the opportunity to get together last year.

I believe that a great deal of activity has taken place, and I would just like to summarize it and perhaps put your mind at rest that we are addressing the problem, and we're doing it seriously.

The Office of Management and Budget has taken its role on computer security and computer management very seriously. In fiscal year 1986, the executive branch expects to spend about $14 billion in general purpose information technology—in other words, computers and telecommunications. This is spread out over 20,000 medium to large mainframe computers and telecommunications systems, and an even greater number of small computers. I cannot tell you how many of your small minis and micros there are but we're getting that information now.

So far, few agencies have taken advantage of the opportunities that have really been offered by modern information technology. More importantly, when they've together plans for their future programs, they have not taken advantage of enhanced information collection, processing and dissemination opportunities they have—in other words, automation. They tend to operate more on a short-term budget basis, which in part can be a byproduct of the entire system—the budgeting system—that works primarily on an annual basis.

So what we have had in the past is, we have not had enough attention paid to long-term planning for ADP processing and telecommunications, and assuring computer security is a very important part of that.

I would also say that the annual budget process—and I depart a little bit, if I may, from my position as deputy Director of Office of Management and Budget—tends to emphasize reduced funds rather than increasing expenditures for enhanced telecommunication and data processing and security. If you are working in an annual process, that's what you'll tend to get.

So agencies will acquire old computer systems, as you know. It is simpler for them to propose patching them and just working with increased operating expenses, then to propose replacing them. In

many cases what you will find is increased technological advancements, which include computer security, will not be proposed because of the difficulty of the process.

I would like to state that one of the problems we've had within the executive branch over the years has been a lack of data in this entire area.

When Peter Grace of the Grace Commission came in several years ago and asked exactly what was our inventory of computers, telecommunication devices, et cetera, we could not tell him, even on a macro basis.

Several years ago, when we started looking at this—and I believe when I came before this committee—I may have stated that we had 17,000–18,000 large- and medium-size mainframes. After we went and did our first full-scale data call this spring, we found out that we had 20,000. It could very easily go up to, let's say, 21, or 22 thousand next year.

The point I'm making is, it would be a mistake to divide out computer security from computer management. They should be intertwined. One of the difficulties we've had is not the fact that we have not had a sensitivity for computer security by itself. We have not had a database to be able to make good management analysis of what is happening within the Federal Government and then apply computer security good computer management. I think we've made some real strides there.

Let me tell you what we've done. First of all, the ORA Office of Information and Regulatory Affairs [OIRA] within OMB is responsible under the Paperwork Reduction Act for developing a 5-year planning process for ADP and telecommunications. This year they Published the second report and sent it to the Congress.

They also sent out procedures for developing effective long-term ADP planning. At the same time, we went out with a requirement getting ready for the fiscal 1986 budget that requested agencies to come send us their ADP and telecommunications systems inventory. We received that this summer.

We have just completed the first management reviews as part of our fiscal 1986 budget review. Mr. Chairman, this has not been done before.

With every single agency, we have very carefully reviewed what we call their information management processes. We focused on five primary areas this year: telecommunications, end-use computing, software management, information management, and electronic filing. In every single case, computer security was considered to be an important part of the overview of the agency.

We next will take the results of our management reviews, and they will become part of the Fiscal 1986 President's budget. This again will be the first time that has occurred within OMB.

What you will see in January will be the first management report that's sent to the Congress. A major part of that will be ADP and telecommunication processing including computer security.

The agencies will then come in with their comments on the overall 5-year planning process. OIRA will again publish the 5-year plan. And the data call will go out to the agencies for next year's budget process. The first update will be done.

By then, we would expect the numbers to start settling down a little bit, and we can come up to the Congress, let's say, by 1985 and be able to give an accurate 5-year plan of what the Federal executive branch expects to do from the standpoint of computer purchasing, computer upgrading, computer security, and everything else related.

So what we've done is, we have taken a major step in institutionalizing the process of reviewing information management within the Federal Government for the first time.

Again, as you know, if you don't institutionalize it, and you do not put it in as part of the budget, it tends to have a very short life in this town. So we think we're taking the right steps.

Also supporting our efforts will be OMB Circular A-123 which implements the Federal Managers Financial Integrity Act. That is not a small effort and it's an extremely important one in the Security area.

This year's report will be the second report that the agencies have sent to the Congress and to the President on their internal control systems after they've conducted vulnerability assessments throughout all of the agencies On the first report, GAO stated in an overview that they thought a very good first effort had been done. I would agree with them.

The second effort that we're going through right now should have corrected many of the deficiencies in internal controls, which includes computer security. I think that those reports that will be coming up in January, will show that much has been done by the Federal agencies on improving their controls.

By using the A-123 process, and combining it with our revisions to circular A-71—which I know you have some interest in—on computer security, we have established the policies and many of the macro standards. And we have worked with the Congress on establishing a process to make sure we are reviewing the vulnerability of Federal agencies to computer fraud.

Mr. Chairman, I'd like to summairze by saying a process has been put in place during the last year that has involved a great amount of work by not only the Offices of Management and Budget, by all of the Federal agencies. We think it stands a very good chance of taking major steps toward correcting some of the concerns and problems you have raised by institutionalizing a management process.

I would be happy to answer any questions you may have.

Mr. GLICKMAN. Let me, again, for the record, try to get an understanding of the numbers of computers, as that term is defined in its broadest context, owned or operated by the Federal Government, and, again, the numbers of dollars that are going to be spent in the next fiscal year on either the acquisition or modification of computers in the Federal system.

Mr. WRIGHT. OK, Mr. Chairman. We estimate there are about 20,000 mainframes that are either large or medium size. I do not have a number for you on the smaller mini's and midi's. We'll get those estimates as we finish the budget process this year. This is the first time we ever called for that data.

As you can imagine, the first time you have a data call, you have definitional problems, and so we're kind of suffering through that.

The amount of dollars that I said are going to be spent in fiscal 1986—and the reason I use that is that it is the time period that we're doing these first management reviews, and we estimate it will be about $14 billion——

Mr. GLICKMAN. In fiscal 1986?

Mr. WRIGHT. 1986. This is what we estimate. It will be for acquisition, maintenance, and operating.

Mr. GLICKMAN. Would there be an equivalent amount roughly spent in fiscal 1985, or are we talking about——

Mr. WRIGHT. I would say that's probably about right; it is in that general area.

Mr. GLICKMAN. And how much of that would you categorize as being Department of Defense related, and how much is non-Department of Defense related, percentagewise?

Mr. WRIGHT. I don't have that number for you, Mr. Chairman. We can get it for you.

Mr. GLICKMAN. OK. Do you have any guesstimate right now?

Mr. WRIGHT. I would say probably two-thirds, if not more than that.

Mr. GLICKMAN. Would be Defense Department related to computers?

Mr. WRIGHT. Right.

[The information follows:]

Based on the President's fiscal year 1985 budget, the Department of Defense will represent 52 percent of Federal, general purpose information technology expenditures in fiscal year 1985.

Mr. GLICKMAN. Does that represent a large increase over, let's say, what it was 4 or 5 years ago in terms of total dollars?

Mr. WRIGHT. Mr. Chairman, I can't answer that, because—believe it or not—we haven't had the data base for 4 or 5 years ago.

My guess is that as you upgrade your technology within the Department of Defense with your more sophisticated systems, yes, it would, but let me see what we can get for you on that.

Mr. GLICKMAN. OK.

[The information follows:]

Department of Defense expenditures for general purpose information technology are expected to grow 65 percent between fiscal year 1982 and fiscal year 1985.

Mr. WRIGHT. Again, a problem we've got in many cases—and this is the entire management area, not just computers—administrative activities tend to get blended in with program activities by account function when we look at it, as proposed by the agencies to OMB, and then as we send it up to the Congress. Until now, we haven't been able to break it out.

Mr. GLICKMAN. Until this year, nobody in Government really had done any inventorying of what information systems there were in the entire Government of the United States.

Mr. WRIGHT. GSA had tried to do some inventorying and I think had done a fairly good job of it. The problem was, the Office of Management and Budget, over the years, had really not instituted separate budget categories for ADP equipment and telecommunications until this last year. That makes it extremely difficult, because you had inconsistency on the data reported by the agencies to GSA.

Additionally, GSA tended to be a procurement oversight as well as a planning assistance organization. So there was no reason, unless they wanted to go into procurement, or they actually wanted to expand their systems for agencies to even go to GSA.

The agencies have reported to OMB because they can't get money even to operate their systems without going through our process. For that reason we've gone on ahead and put the management review process, for the first time, into the budget process.

Mr. GLICKMAN. Now, who is in charge of issues relating to acquisition, management, and computer security of computers in this Government? If I were to ask you, Mr. Wright, who do I talk to about, let's say, improving computer security issues in the Department of Agriculture or the Social Security Administration? I mean, who do I talk to? Who is in charge?

Mr. WRIGHT. We do not have anybody specifically in charge of computer security, which I believe is what your question is.

I'm not sure that we should have somebody in charge of that, because, again, I look upon computer security as part of computer management. I do not believe that we ought to have one person out there that is responsible for proposing what the improvements are going to be within a computer program and another person out here totally separate that is responsible for computer security.

Mr. GLICKMAN. Well, then, who's in charge of computer management in the Federal system?

Mr. WRIGHT. Two parts of this: I would say the person who is in charge of the overall management reviews for the Office of Management and Budget is Arlene Triplett, who's the Associate Director for Management. She shares that responsibility in the computer area with Doug Ginsburg, who is the Administrator of the Office of Information and Regulatory Affairs. He is responsible under the Paperwork Reduction Act for the 5-year ADP planning process.

Mr. GLICKMAN. But it's then—it's the Office of Management and Budget——

Mr. WRIGHT. That's right.

Mr. GLICKMAN. That would be responsible for this.

Mr. WRIGHT. That's right.

Mr. GLICKMAN. And I'm trying to figure out what your relationships are with the other Federal agencies and/or GSA.

You know, you talked about in your statement—to your OMB Circular No. A-71 entitled "Security of Federal Automated Information Systems," but once you get that circular out, what then happens? Is it in the form of a—let's say, a regulatory order to these agencies to comply, or do they—is it an advisory circular?

Mr. WRIGHT. OK. A-71 is primarily an advisory circular, but it does establish firm responsibilities of the agency heads. Part of our responsibility is making sure that computer management and computer security is on their shoulders in their agencies and departments.

Our relationship with the other agencies is fairly simple. We are the coordinator that sends out the overall policy and makes sure that everything that I've mentioned happens, from vulnerability assessments to overall ADP policy, to putting ADP planning, including computer security, into the budget and the management report that comes up to the Congress.

GSA is working very closely with us on this, and they will pick it up from the procurement side and support us also on the planning side. They're playing a major role.

The Department of Commerce, that you were with this morning, is also playing an important role in developing standards, and they've already published several documents on computer security and what those standards are.

The Office of Personnel Management is also playing a role in developing training sessions for computer security, and they're doing this along with several outside organizations.

But if you want to take the one agency that's responsible for tying it all together, it's the Office of Management and Budget.

Mr. GLICKMAN. Well, once your guidelines on computer security are updated, what followup do you plan to ensure that the agencies comply, and do you have adequate staff and expertise to do that?

Mr. WRIGHT. Yes, sir; I believe so.

We will, first of all—agency activities will be reviewed within the A-123 process. Vulnerability assessment are going to be done by every single agency. A key part of that oversight is the inspectors general. You're going to have Mr. Kusserow testifying before you shortly, and he can best describe that. They are part of the President's Council on Integrity and Efficiency, of which I am the chairman, and we play a major role on that whole A-123 process.

Second, we will be developing the 5-year ADP plans, of which computer security will be a part.

Third, we will undertake the second year data call on ADP and telecommunications. Then we will conduct the second management reviews as part of the fiscal 1987 budget, and then we'll put those results into the next President's budget. So they all fit together in our oversight process.

I guess I might add, Mr. Chairman, just very briefly, there's more than just the Office of Information and Regulatory Affairs that is responsible for this area. This year, by establishing the management reviews, we got the entire management staff involved in it as well as the budget staff of OMB. That hasn't happened before.

Mr. GLICKMAN. How much time of this Office of Information and Regulatory Affairs do you think is spent on the issues regarding computer security?

Mr. WRIGHT. I would imagine that there's not too much by that particular office itself, but by the entire staff of the Office of Management and Budget I would imagine there is quite a bit, because this is the first year we've done that. This is the first time they've had to get in this entire area with good data. I can't give you a number on it, but I would say the overall time that is devoted to this subject within the Office of Management and Budget, my guess, has gone up dramatically during the last year.

Mr. GLICKMAN. I go back to the issue of followup, because reports of continuing computer fraud and abuse suggest that the followup to ensure that the agencies are complying is really long overdue, that there hasn't been any followup for at least 5 or 6 years.

Mr. WRIGHT. OK——

Mr. GLICKMAN. And of course the numbers of computers have just increased dramatically and the sophistication of them.

Mr. WRIGHT. That's right.

Mr. GLICKMAN. And somebody has to be in charge of at least ensuring that followup on computer security is being done. Let me give you one of the things that concerns me.

A recent article of Government Executive magazine states that the Treasury Department and the Federal Reserve system are in the forefront with regard to protecting their computer systems. Others are much less concerned; the article goes on and describes those. Concern may be—just relative to the level of people and personnel who are involved in this thing.

So I'm telling you that there are some agencies that—perhaps affecting the banking system—that see this problem perhaps in a more acute way, and others don't, and notwithstanding what their inspector generals are talking about, there's got to be somebody on top who, as you say, are involved in the management of these systems pushing them, or else people's records in those agencies are jeopardized—the privacy of those records.

Mr. WRIGHT. Individually within every agency, it's the agency head, but let me add one more thing that is kind of beyond that.

I guess, since all the staff that are involved in this, with the exception of the outside agencies that are assisting as, report to myself, that I would say the Deputy Director of the Office of Management and Budget is responsible for making sure that all of these reviews are conducted in a timely and a professional fashion, and that they have—if you want to call it—the strength and the severity of the budget exercise behind them.

So as we have institutionalized the process, I am staying on top of this process every step of the way and will do through the next year.

Mr. GLICKMAN. OK. Well, let me—one suggestion might be that each agency reports to you about unique problems associated with the operation of its computers and ways that computer security may be different from agency to agency.

Example: "20/20" did the story about the FBI's Crime Computer, where people who get in there, either by mistake, or the information isn't pulled out—in some cases, innocent people are kept incarcerated for a period of time because the information is old, is not accurate, or is improperly inputted.

That's an example that may affect the FBI; and, by the way, every crime control center in the U.S. police departments, sheriff's departments, depend on the accuracy of that information. That's different than maybe what may happen in the Internal Revenue Service or the Social Security Administration.

If you're not aware of the problems—what are the potential problems, then computer security may be kind of an abstract exercise, and what I'm telling you is that each one of these agencies may have unique problems, where its computers may be inputted improperly or accessed improperly or just not operating in the way they're supposed to be, that somebody on top has to be aware of, and I'm convinced that maybe there's not total unanimerity of interest there, where it may not be the Justice Department's interest to correct this quite as quickly.

It may be your interest to make sure it's corrected; and I'm suggesting to you that one of the things you may do in lieu—not in

lieu of but in addition to this circular, is bring together the heads of the agencies or their appropriate designees, and sit down and talk about the unique aspects of each particular agency and how it uses and deals with its information in its computer systems, and begin to exchange that information to take care of some of these problems that we see once in a while like on "20/20" and elsewhere.

Mr. WRIGHT. Mr. Chairman, I agree with you.

In many cases, there is not the same interest—there's no question about it. It is not unique for the Office of Management and Budget in their role to disagree with the line agencies. So we feel very comfortable in that, let's say, adversarial position.

I would add that we did bring the assistant secretaries for management who now constitute the President's Council on Management Improvement together, and we have made it very clear to them that they've got a major role in this area.

That is patterned—that council is patterned after the IG's and the PCIE, where there is a little bit of a dual reporting relationship, albeit daunted, up to the Deputy Director of OMB, who is also the chairman of that council. We are going to be using that council as the primary group for implementing many of the changes I've talked about and to make sure that process goes in place that I just laid out.

In order for that process to work—and I'd say we're half-way through it right now in the first year, and I'm very pleased with the way it's worked so far—we're going to have to dog it every step of the way; no question about it.

Mr. GLICKMAN. OK. Let me ask you this. Who in the Government has the responsibility for overall guidance with respect to protection, let's say, from terrorists or disgruntled employees of nationally important computer-based systems, both Government-operated and private sector—for example, the air traffic control system; the electric power generation grid in this country? Who in Government has that responsibility to help either its own computers or help the private sector deal with the issue of protecting those systems? Is that you? Is that FEMA? Who?

Mr. WRIGHT. OK. On the nonnational security areas, that is primarily the agency head's responsibility as designated to him or her through the A-71 process. This is for Federal——

Mr. GLICKMAN. So, like what? Air traffic would be the FAA?

Mr. WRIGHT. That's right.

Mr. GLICKMAN. What about electric power—the grids in this country? I wonder who'd have responsibility for that. Those are all computer-connected as well as computer-generated.

Mr. WRIGHT. Do you know——

Mr. BEDELL. That would be——

Mr. GLICKMAN. Would you state your name for the record?

Mr. BEDELL. Yes. I'm Bob Bedell. I'm the Deputy Administrator of the Office of Information and Regulatory Affairs at OMB.

That would be primarily the responsibility, again, of the Department of Energy. This time—and like the other departments and agencies, they would be operating in accordance with and under the constraints of the policy issued by the Office of Management and Budget and the other central agencies in seeing to the security

of these systems, but primarily the responsibility would rest with the agency head concerned.

Mr. GLICKMAN. OK.

One of the things that I am contemplating in the next Congress, although it's too early now, is some sort of a computer security institute or some more specific computer security training mechanism in the Federal system, perhaps involving the National Bureau of Standards, but not in the kind of loose fashion that exists now where some agencies really just do nothing and some agencies, as I said, like the Treasury Department, are heavily involved in the issue—all to provide awareness, training, and assistance in implementing security controls to Federal agencies. I wonder how you'd feel about that.

Mr. WRIGHT. Mr. Chairman, now that you mention the ICST as a vehicle that might do that, I think that could be a good idea. I believe that they are doing some good work in that area.

I'd say that there is no question that the work they're doing could get expanded coverage and distribution throughout the Federal Government, and we could work with them.

And with OPM and through OMB to make sure that happens.

I would say to establish another independent group separate from them probably would not be a good idea, because you'd be kind of inserting them right in the midst of the overall process, and it would be a little confusing.

You have the components in place to make the process work that I just mentioned to you between OMB, GSA on the planning and procurement side, OPM on the personnel planning side, and the Department of Commerce on the standards side. So now let's take and kind of play with those four factors. If we need to beef something up or improve the coordination through the PCIE with the inspectors general, through the PCMI with the Assistant Secretaries or about implementation of A-123 on the vulnerability, we do something to beef it up one way or the other. Let's play with it, but I would not create an independent organization.

Mr. GLICKMAN. Do you think there is a need for an integrated Federal database with uniform definitions on computer crime?

There seems to be a lack of—of uniform descriptions and definitions of what that is, and so we don't really know what—who is being ripped off and who isn't, and one of the problems we've had in this whole area has been the lack of that integrated database.

Mr. WRIGHT. I agree; I think it has been a problem; and earlier this year, I asked the inspectors general to go and take a look at that and see whether or not we shouldn't establish a Federal database on computer crime.

Inspector General Kusserow, who is coming up, can tell you the progress that has been made on that, because he's been in charge of that task force.

While they do not have a full database on computer crime—and, by the way, I'm not so sure that a 100 percent database would do that much good for you—they have made some pretty good progress, and he can describe that to you.

So I would agree with you, and we asked them to do that earlier this year.

Mr. GLICKMAN. You know, you've responded to the committee report, and I understand some of your concerns about some of the things that we've talked about here, but on page 8 of your statement, you talk about—that—we talk about the fact that the problem of computer security is one that requires a national solution to it.

We don't—we're not terribly specific about what that solution necessarily is, but you put in your statement, "It is unlikely that Federal guidance from Washington could solve such unique and diverse management problems. Furthermore, it sets a dangerous precedent for Federal intrusion into private sector areas in which it does not belong."

Well, we have intruded already. We've passed privacy statutes which protect the information so that the owner of that computer can't give that information away, or else violate the law.

What I'm saying is, and what we've been saying is—is that information can be exploited and disseminated without the owner's knowledge and consent, and I hate to have you say that it is not a national problem when it looks like to me the Federal Government, with its 20,000 computers, many of which are tied in with the private sector, and the lives and security of people who are affected by those things do depend, in some respects, on the national Government to provide research and development, help with the private sector, and in some cases direct solution because its own computers are involved.

Do you mean to imply that there is—you know, on the one hand you're saying you're getting your regulatory house in order; on the other hand, you say you hate to see the Federal Government intrude in the private sector in areas where it doesn't belong. I tend to think that there is a dichotomy between those two positions.

Mr. WRIGHT. OK. I guess I'm trying to take a little bit of a philosophical as well as a practical approach toward it.

First the practical side. We have so much work to do to get our Federal house in order right now and just make sure this process is implemented properly, so that by the the year 1985, we can come up as we're going into the third year on the entire process I described, and say, Mr. Chairman, we do have a 5-year plan that I've got confidence in. And it includes not only computer management but computer security as well—in both the mainframe and also in the telecommunication networks.

That is a major, major task. And we should certainly focus on that.

The second point is that you get into this fuzzy area of Federal and non-Federal responsibility. Federal agencies have an overwhelming propensity to try to get into the private sector, if they possibly can. I would humbly say that from a philosophical standpoint, we ought to be very, very careful before we start establishing standards for the private sector, unless we are absolutely sure that they are in the national interest for safety, for overall privacy or a national basis, and for security.

Mr. GLICKMAN. OK. I have one final—go ahead.

Mr. BEDELL. Excuse me. I just wanted to add that with regard to most of the Federal privacy legislation, it has dealt only with Federal systems. The Federal Privacy Act itself does not address pri-

vate, nongovernmental systems at all, and the Congress in 1974, and subsequently in considering privacy legislation, has gone out of its way to make sure that the Federal Government didn't get involved in trying to set standards for or regulating the private sector with regard to——

Mr. GLICKMAN. Well, but we are beginning to move, and, in fact, we passed a computer crime bill out of the House which made it a crime to improperly access a computer for credit purposes.

So, you know, as far as the individual is concerned, the information that's stored in those computers, whether they're Federal computers or whether they're credit bureaus' computers, are similar.

I'm not saying that Uncle Sam ought to come in and take over the security of private computers, but there is obviously some continuity of interest there, and I'd hate to see you take a philosophical view of the need to protect information stored in computers, because there's a lot the Federal Government is already doing with the private sector at the National Bureau of Standards and other places, and I don't sense today that you want to eliminate that work that's being done at the NBS.

Mr. WRIGHT. No, not at all.

And, by the way, I would say that as we get through this process, when we can give you a better feeling of exactly what is in the Federal inventory, and where the weaknesses are, and where they are not. Then we might be in a better position to say whether we should expand it or contract it.

Mr. GLICKMAN. OK. Final question: How would you characterize, Mr. Wright, the overall level of computer security awareness and the implementation of computer security safeguards in the Government today?

Mr. WRIGHT. I guess you have to say how you are doing today, compared to what?

Compared to the last several years, I guess when you and I first started talking about it, I would say the awareness is heads and shoulders above where it was then, due in no small measure to the fact that it has been discussed several times in Cabinet meetings with the President when the Cabinet officers were told, as part of the Financial Integrity Act, that they were going to have to personally sign the reports on internal controls to the Congress and to the President. That kind of got everybody's attention, to begin with.

Since then, that entire process that I have mentioned to you has been put in place in a very short period of time by Washington, DC, standards.

As you know, to put any process in place that begins to work in this town in a period of a year or two is really phenomenal progress. And you have two councils—Presidential councils that have been set up to deal in this area of fraud, abuse, and control of management and administrative systems.

So, I would say that awareness has gone way up.

Mr. GLICKMAN. The awareness is up. How about the implementation of computer security safeguards itself?

Mr. WRIGHT. I would say that implementation is occurring while we are sitting here, and it's probably occurring at a faster rate. The difference will be that next year when I come in, I'll be able to give you some numbers. We've never been able to give numbers

before. Also the difference will be that technology management is going to be specifically identified as part of the budget this year, because we have separated out the management reviews as part of the budget exercise.

Mr. GLICKMAN. OK. Well, we appreciate your testimony. We'll be in further contact.

I'd like you to consider again my suggestion that you bring in particularly the relevant agencies who have computer systems with peculiar problems and ask them to sit down among themselves and talk about those problems, because they're very much a concern to the American people. Finding their names in the crime data bank and can't get them out—I mean, that's obviously a concern to a great number of people, and sometimes it takes the superiors, the people from the outside, to focus in on those things, and that's an area of computer security as well, accuracy of information contained therein.

So, we appreciate your testimony, and we'll be in contact with you in the future.

Mr. WRIGHT. Thank you, Mr. Chairman.

[The prepared statement of Mr. Wright follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR RELEASE ON DELIVERY
Expected at 1:30 P.M.
Monday, September 24, 1984

STATEMENT OF JOSEPH R. WRIGHT, JR.
DEPUTY DIRECTOR OF THE OFFICE
OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS
OF THE COMMITTEE OF SCIENCE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES
ON OMB'S EFFORTS TO IMPROVE FEDERAL COMPUTER SECURITY

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss OMB's continuing role in computer security. We have long been interested in assuring the security of Federal automated information systems. According to your letter of invitation, the purpose of this hearing is to solicit comment on the Subcommittee's recommendations in its report, "Computer and Communications Security and Privacy" (April 1984) and to update the Subcommittee on recent developments in computer security. Therefore, I will not review the various Federal agency activities concerning computer security set forth in my testimony before this Subcommittee on October 17, 1983. In particular, you asked that we report on our management initiatives to oversee the Federal agencies in implementing security measures and our effort to consolidate and update policy circulars relating to Federal information resources.

When discussing computer security, it is useful first to clarify what we mean by that term. Computer security means (1) protecting the computer or data while it is within a computer or communication system but also (2) assuring that computer systems do exactly what they are supposed to do, and nothing more. So when I speak of computer security, I mean a system of management controls to ensure the integrity of computer operations including such matters as proper access to the information in the system and proper handling of input and output. And I mean assuring that controls in computer applications are working so they properly perform their function.

Unfortunately, to some people -- particularly managers -- the term "computer security" has had a narrow technical meaning. As a result, some believe that assuring adequate computer security is the responsibility of computer technicians. Often this results in seeking a technical solution to what is really a management problem.

In my testimony last year, I discussed the growing dependence of the Federal Government on computer and communications technology. That trend, if anything, has accelerated and become more apparent. There are now more than 20,000 medium and large scale computers in the Federal inventory. We expect to spend nearly $14 billion for information technology support in fiscal year 1985 -- which accounts for 1.4% of the total Federal budget.

With this growing dependence, our concern for adequate security of those automated systems has increased. The Subcommittee's report draws attention to this important issue.

Last year, I discussed the findings of the President's Council on Integrity and Efficiency's initial report on Federal computer crime. At that time I said that most instances of an absence of adequate computer security would not be due to a lack of adequate tools, but to a combination of lack of knowledge of those tools and lack of understanding by managers of the need to use such tools.

Therefore, we have undertaken a two part approach to enhance Federal computer security by:

(1) Clarifying responsibilities for security in revised policy guidance; and

(2) Raising security consciousness on the part of those who design, maintain and use automated systems.

As part of a revision of four OMB Circulars, Transmittal Memorandum No. 1 to OMB Circular No. A-71 entitled, "Security of Federal Automated Information Systems," is in its final stages of being revised by a task force of OMB and agency personnel with substantial experience in computer security. We expect to release a draft for public and agency review in the next few

months. This revision will include a clearer delineation of responsibilities for the security of automated information systems.

On August 16, 1983, we released OMB Circular No. A-123 implementing the Federal Managers' Financial Integrity Act (P.L. 97-255). It prescribes policies and standards for departments and agencies in establishing, maintaining, evaluating, improving and reporting on internal controls in their program and administrative activities. During the past year, Federal agencies have put forth a substantial effort to evaluate the vulnerability of their programs and to take measures to reduce their vulnerability. At the center of these efforts has been an evaluation of the automated information systems that support those programs.

Because of those evaluations, several weaknesses in automated agency systems have been identified and corrected. Within the General Services Administration's automated supply system, for example, weaknesses were identified in controls over systems access, separation of duties, and edit checks on input data. GSA has already corrected weaknesses concerning access to supply records by separating the duties of key employees. They plan to implement edit check procedures later this month.

The Department of Agriculture reported that the Farmers Home Administration's automated balancing procedures and controls in the Finance Office's accounting system were insufficient to ensure that data entered into the system is properly recorded. The Department will correct this weakness in the automated balancing procedures by changes to the existing system after conversion to an adequate mainframe.

The Department of Transportation found that it had no department-wide inventory of sensitive computer applications nor did it have a program for certifying computer security safeguards. Also, risk analyses of ADP centers were not being performed on a regular basis. The Department now requires all of its administrations to develop an inventory and a schedule for certification. The Office of the Secretary is developing a schedule for performing risk analyses of all computer facilities.

I should note that in some agencies we found considerable uncertainty as to how to conduct vulnerability assessments in their automated programs. We are working with those agencies to develop guidance for measuring and reducing that vulnerability. Recently we published a list of 50 commonly asked questions and answers about the OMB Circular No. A-123 risk management program, including its relationship to computer security programs, to assist agency managers in implementing internal control systems.

In addition, the President's Council on Integrity and Efficiency is updating their initial study that we discussed last year. I understand that the Inspector General of the Department of Health and Human Services, Richard P. Kusserow, is scheduled to testify before the Subcommittee to discuss the Council's findings.

The Subcommittee's report, "Computer and Communications Security and Privacy"

With regard to the specific recommendations in the Subcommittee's April report, several of the activities we have under way to enhance the security of Federal automated systems are consistent with the Subcommittee's recommendations. For example, the Subcommitee recommended expansion of training of existing manpower to improve computer security programs, including the training of non-technical personnel. As I noted above, we have heightened security awareness in the Federal Government and we support efforts to enhance security training of Federal personnel, both technical and non-technical.

We believe that it is beneficial for Federal agencies to share security expertise and techniques with the private sector and for the private sector to share such information with the Federal agencies. For example, we have much to learn from the private banking community in securing Federal financial systems. Similarly, there are aspects of communications security such as

techniques for preventing electronic eavesdropping in which the Federal Government has substantial expertise of value to private concerns.

A National Commission

The Subcommittee recommended the establishment of a national commission to examine the issues surrounding the security and privacy of computer and communications systems. While it is difficult to provide detailed comments on this recommendation without a specific legislative proposal to evaluate, it raises several concerns that are not addressed in the report:

1. The report does not demonstrate the need for a national commission on computer security. As the findings of the report indicate, "Information systems and processes along with the data contained within them represent assets of incalculable value to their owners and to the society at large." That finding while often correct does not demonstrate that we need a Federal commission. What it does indicate is that there are strong incentives for managers in the public and the private sector to secure their systems without a Federal commission telling them that they should.

2. The report does not demonstrate that there is a problem that requires a national solution. While the report states that "...intentional and unintentional threats and vulnerabilities of these resources are real and therefore present a problem of national significance," the report cites as examples a diverse set of unique systems. The security problems of unique systems require unique solutions, particularly since most computer security problems are management problems. It is unlikely that Federal guidance from Washington could solve such unique and diverse management problems. Furthermore, it sets a dangerous precedent for Federal intrusion into private sector areas in which it does not belong.

3. It is overly optimistic to assume that a commission could deal with all of the subjects described in the report. The report notes that these subjects include "...an array of multifaceted issues including national security and defense, vulnerability of critical systems, the effect of technology on privacy, computer-related crime, and the social and political consequences of intensive computerization." It goes on to say that "...because of the complexity ... of these issues, it is unlikely that any single Executive Branch organization or Congressional Committee will be able to deal effectively with them all." Given this level of complexity, we believe it is overly optimistic to assume a study commission could analyse these questions in any meaningful depth and provide new and practical recommendations.

4. We and the Federal agencies are actively moving to enhance security of Federal automated information systems A national commission should not impede those efforts, or provide a basis for delay.

A "Central Focus" to provide technical assistance

The Subcommittee's report also recommended that OMB establish a central focus to provide technical assistance to agencies that are responsible for sensitive, non-national security data in selecting tools and techniques to protect their computer systems. We agree with the Subcommittee that Federal agencies need a source of technical expertise to assist in implementing security measures. However, such sources already exist both at the National Bureau of Standards and at the DOD Computer Security Center. Furthermore, such expertise is readily available in the private marketplace. Therefore, we are not convinced of a need to establish another center at the Federal level.

We believe that the Federal Government should continue to make available information on computer security matters for those accountable for Federal systems. For example, the Institute for Computer Sciences and Technology at the National Bureau of Standards is developing security "tools" and working to enhance security awareness. They have published several Federal Information Processing Standards on various aspects of computer

security. They have established a data base of security "enhancements" for Federal managers concerned with securing their systems. Later this month ICST will publish a guide on small systems security. Additionally, they provide consulting assistance on security to many departments and agencies.

As I discussed earlier, we at OMB are completing the drafting of a revised OMB Circular that will cover computer security matters. Furthermore, we are closely monitoring agency progress in assessing the vulnerability of their systems to assure that they take action to minimize fraud and abuse resulting from inadequate controls on those systems.

Establishing a Non-defense Classification System

The report recommends that OMB establish a non-national security data classification scheme to protect categories of sensitive data (e.g., financial, medical, inventory systems) in the Federal government. We question both the utility and practicability of such a scheme for several reasons:

1. Information systems should be secured commensurate with the risk and magnitude of loss or harm that could result from their improper operation. This harm test, established in the Privacy Act of 1974, requires judgment on the part of the individual responsible for the security of information. Defining

categories of sensitive information (e.g. financial, medical, inventory information) and protecting all information in a category at the same level, removes that judgement. All financial information, for example, should not be protected to the same degree.

2. Defining categories of data to be protected defines the level of security to be provided out of context of the specific information. For example, a name and address are personal data, yet depending on what information is connected to the name, they may be highly sensitive or not sensitive at all. Similarly, certain information is only sensitive if prematurely released (e.g., crop forecasts).

3. Where there are categories of data needing protection, the Congress provides statutory requirements for protection (e.g. tax information, national security information, personal information). Defining an additional comprehensive set of data categories would tend to confuse and complicate, rather then simplify.

4. It promotes the wrong incentive. The responsible individual would need only protect the system according to the guidelines for that category to fulfill his or her obligation, regardless of what the risk of loss or harm is for that specific system. There would be little incentive to provide additional security.

Furthermore, other systems would be protected much more rigorously than their true risk would warrant, simply because of the category of information processed.

We share the Subcommittee's concern that Federal automated information systems be properly protected. The sole purpose of Federal information technology is to effectively and efficiently carry out governmental functions. Assuring proper levels of security during the processing in such systems is essential to that purpose. Therefore, let me reiterate that we in OMB have a high and continuing interest in the security of Federal automated information systems.

I would be pleased to answer your questions.

Mr. GLICKMAN. Our next witnesses are Mr. Bruce Campbell and Mr. Frank Carr, Emergency Mobilization Preparedness Board.

Mr. Campbell, you are with FEMA—correct?

Mr. BRUCE CAMPBELL. Yes, sir.

Mr. GLICKMAN. And Mr. Carr, you are with GSA?

Mr. CARR. That's correct.

Mr. GLICKMAN. OK. Well, we appreciate your being here.

Mr. Campbell, I had the opportunity of riding in the airplane with the director of FEMA, and it was a very enjoyable meeting. We talked quite a bit about some of these issues; but anyway, you may, again, read your statement or summarize your statement, as you deem appropriate.

STATEMENT OF BRUCE CAMPBELL AND FRANK CARR, EMERGENCY MOBILIZATION PREPAREDNESS BOARD, EXECUTIVE OFFICE OF THE PRESIDENT

Mr. BRUCE CAMPBELL. Yes, sir.

Mr. Chairman and members, we do have a prepared statement which we would request to submit for the record, and I'll do a summary and then be prepared to answer questions.

As you said, I'm from FEMA; my distinguished colleague, Mr. Carr, is from GSA, and we find ourselves representing the National Security Council, particularly Mr. Robert McFarlane, the assistant to the President for national security affairs, and the Emergency Mobilization Preparedness Board.

We cochair the Task Force on Automated Information Processing, or AIP, for the Government Operating—Operations Working Group under this board.

We also appreciate the opportunity to speak to you today concerning this subject, and we also consider it to be of vital importance to our Nation's interests—more specifically, the survivability of our governmental process.

The Emergency Mobilization Preparedness Board, or EMPB as it is referred to, was established by President Reagan on December 17, 1981. The purpose of that board was to ensure that the Government has the capability to provide for the security of the Nation and to protect its people, values, and its social, economic, and political structure, and to assure that Government at all levels, in partnership with the private sector, can respond rapidly and effectively to any national security or major domestic emergency.

The Board, as chaired by Mr. McFarlane, consists of representatives of 23 key Federal departments, agencies, and executive offices at the deputy or under secretary level. This, again, goes in line with what Mr. Wright had said, illustrates the progress of things in this particular area.

The Board normally meets quarterly, and its basic charter requires it develop an overall mobilization preparedness policy as well as a plan consistent with that policy to improve the Nation's capabilities.

The Board's policy formulation is carried out by working groups in 13 functional areas. One of the those is Government Operations Working Group, which is chaired by FEMA.

The interest of this group in AIP was generated by another functional working group, which is the Emergency Communications Working Group, on which both Frank Carr and I sit as members.

That AIP problem was initially identified in terms that the committee is also concerned about—the increasing reliance on AIP in the key support areas, both government and industrial operations—and this increasing dependence, we also feel, renders us rather vulnerable in the event that AIP supporting the National Security Emergency Prepardeness Functions is impaired or lost.

Adding to this particular problem of NSEP are the unique considerations contributing to the Federal AIP problem, a lot of which you have heard in Mr. Wright's testimony and the answers to your questions, Mr. Chairman.

To add to those examples, the computer and telecommunications equipment and systems in this Federal Government inventory have been supplied by 1,000 or more vendors, including a lot of equipment that is currently obsolete by GSA standards.

Further compounding the problem is the continuing and rapid proliferation of the new information processing equipment and systems products such as the word processors and the personal computers. We refer to these equipment resources, when you add them to the personnel resources, as making up our AIP infrastructure.

This led us to the development of the definition of AIP which we are using in the task force. Simply stated, it is the collection, storage, manipulation, presentation, and distribution of data, primarily by machines, to provide information needed to support management decisions and operations.

We also consider AIP to be a part—a critical part of information resources management, or IRM, which encompasses all the automated and manual handling of data, including computer processing as well as telecommunications.

The Emergency Communications Working Group reviewed this problem and proposed that the thrust of the board effort should be to reduce this vulnerability that would result from the Nation's dependence upon AIP by carrying out Government and private sector planning in support of emergency operations instead of focusing on the security, survivability, and endurance of resources used to support normal operations.

After briefings and considerable discussion of these alternatives by the EMPB board members, it was decided that this initiative would be retained at the board level with the Government Operations Working Group directed to establish the subworking group which Frank and I chair—cochair.

We would assemble the necessary expertise from interested agencies and work the problem while coordinating with the reform-88 project and a number of the things that Mr. Wright had talked about at the OMB level.

The AIP task force was formally established. Membership presently consists of nine Federal agencies that have essential emergency functions as well as a key interest in this issue.

The Department of Defense, Commerce, Transportation, Justice, Agriculture, Treasury, as well as the Veteran's Administration are on this subgroup.

39-741 O - 84 - 3

Our first assigned task is to develop particular guidance for the Federal departments and agencies toward assisting them in developing their own plans for the use and protection of AIP in emergency situations. When completed, this guidance will be distributed to all the Federal agencies and departments in a Federal preparedness circular.

To demonstrate the tie-in between the Government and the private sector activities in this area, the AIP task force is also coordinating with an AIP task force in the private sector, which was created by the National Security Telecommunications Advisory Committee—or NSTAC—to the President. This was established in September 1982, under Executive Order 12382.

This NSTAC AIP task force is made up of 11 major companies representing elements of the telecommunications industry. Their initial efforts were to identify and scope the issues critical to establishing this framework for joint Government/industry planning and toward approving the survivability of AIP capability which supports national telecommunications systems.

In the past, emergency preparedness efforts within both the private sector and the Federal Government have usually been identified principally with providing back-up facilities in the event of equipment failure or loss of capability because of fire, flood, earthquake, or other emergencies.

Contingency planning for AIP, we feel, is not simply a matter of identifying certain functions performed in peacetime as critical under emergency situations. It requires an understanding of how the emergency situation modifies the agency mission and the consequent decisions support information required.

As a concerted effort, under this AIP task force, we hope to achieve several significant goals in support of these—of national security emergency preparedness. One is establishing an awareness within both private industry and the Federal Government of the criticality of certain AIP systems.

This goes along with the committee's view toward the awareness question—developing methodologies and procedures for identifying and assessing the vulnerabilities of these AIP systems, developing methods for identifying AIP deficiencies and requirements, establishing the framework for a survivable infrastructure to support these critical systems.

Infrastructure resources include such categories as the key components you had also mentioned to Mr. Wright: the energy, including the electric power and environmental systems; transportation for personnel; the maintenance, parts and services; communication lines and systems; personnel as well as the food, water, and health services to support these personnel; civil security protection, such as the police and fire; and so forth.

As you can see, describing this overall infrastructure to support NSE—National Security Emergency AIP can become extremely complex, and this is what our AIP working group is about.

As you can see from these and varied actions initiated with the participation of the Federal agencies and departments as well as FEMA's overall mission responsibilities, we have been making significant progress toward improving this overall AIP posture of the Federal Government.

We believe these steps will contribute to ensuring that information resources are acquired, enhanced, utilized, disposed of, and protected in cost-effective ways while achieving the Federal Government's goal.

Mr. Carr and I thank you for the opportunity to present this information to the subcommittee, which we believe are significant steps toward improving computer and communications security in support of national security emergency prepardeness functions and programs.

We'd be pleased to respond to any questions.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you.

Mr. Campbell or Mr. Carr, tell me, how vulnerable is this Government or our country, and what are the consequences of a major computer disruption? That is, are we vulnerable in the air-traffic area? Are we vulnerable in the electric grid area? Are we vulnerable in the banking area? And I'm not talking about if a terrorist going to do something tomorrow. Are the systems vulnerable?

Mr. CARR. I think you would have to say that almost every computer system is in some way vulnerable. We can answer part of your question that way, but the question—the other part of it, which was how much is the thing you really can't put your finger on.

You know, I can't help but liken it to the bombing of the embassy. Every embassy in the entire world is vulnerable. The issue really becomes one of degree of protection, how you plan for it, and what your attackers may consider doing.

The situation we really find ourselves in, I think, is one that over the past, let's say, 30 years ago, we didn't have any problem, because we didn't have any computers processing data. We created the potential as we began to use computers; we increased the potential as we began to access computers remotely; as vulnerabilities increased, we began to find better defensive mechanisms, and those have been introduced.

Mr. GLICKMAN. It strikes me that the—the computers and the information systems have increased far more rapidly than the defensive measures to protect those systems.

Mr. CARR. I don't believe that is true. I think the defensive mechanisms are there.

I think it gets back to the issue of the application. The very question and the very type of thing that I think you said—the specific problems that you have in specific agencies, you have to take that specificity, not simply down to the level of the computer system but to the level of the application that's being brought on that system.

Mr. GLICKMAN. Let me take an example. Have you—either of you—worked with the FAA? We're going to be spending $10 billion on the largest nondefense computer system in this country in the next 10 years. Anybody working with the FAA to determine the viability, protectability, defensibility of that system?

Mr. CARR. We have—I have not worked with the FAA on that specific issue, but we have worked with the FAA on the general problem of planning for those systems, and part of that planning involves making that kind of an assessment, and that is built into our management system.

You mentioned A-71, which is the basic document that outlines responsibilities. You have NBS that establishes the basic standards. GSA, in its regulations, places that requirement specifically on each agency. Public Law 96-511 establishes a senior official in each agency who is responsible for implementing those regulations.

Then you drop down to the people who actually have to determine the system they want and the specific requirements that have to go into the system, and it's at that level that the problem really gets dealt with, when you get down to the—

Mr. GLICKMAN. Or doesn't get dealt with.

Mr. CARR. Or it doesn't—either one, but you have to get down to that level when you state the requirement: What is the system to do? What is the accuracy required of the data? What's the timeliness requirement? What security is required?

Mr. GLICKMAN. Well, let me ask you this. Are you aware that we're talking about buying $15 billion worth of computers a year? Are you aware that in any of the RFP's or any of the actual discussions that occur between vendors and the Government that computer security is a key part of the acquisition process?

Mr. CARR. You say "key part." I can't address the word "key," but certainly it is a part.

Mr. GLICKMAN. Well, I mean is——

Mr. CARR. It is a part. It's included in the RFP's.

Mr. GLICKMAN. The protectability of the system. I've seen some, and I haven't even seen that language in there. Now, maybe it's new that they're beginning to think about that.

Mr. CARR. You'll find that, for example, in the acquisition of time-sharing services; you'll find it in contracts for system development; you're also going to find examples where that is not included; you'll also find a lot of examples where the basic things I talked about, irrespective of the security issue, also aren't being addressed.

Mr. GLICKMAN. Well, let me ask you this. OMB said that each agency is responsible for protecting critical national systems: the Department of Energy, electric grid; FAA, air traffic; we can run down the list of—Federal Reserve Board, maybe electronic funds transfers. Does your board have any responsibility for providing overall guidance?

Mr. CARR. The group that we're responsible for is basically looking at a fairly narrow question, of which security is a part.

What we're concerned with is the planning for automated information processing systems to support Government operations during specific types of emergencies or national security—full mobilization, for example; what kind of information processing do we need at that time?

Now in the planning for that information processing, one of those requirements would be the heightened possibility—increased possibility of sabotage efforts during that period. That would be a requirement that would be addressed in determining what that system has to be able to do.

Mr. GLICKMAN. Well, I think planning for full mobilization is an interesting phenomenon, but I think far more likely is damage to national systems from many other kinds of things.

Mr. CARR. That may be very well true.

Mr. GLICKMAN. Terrorists, sabotage; I don't want to see you so planning for the invasion of this country by the Soviet Union that we don't deal with the kinds of things that are actually more likely to occur.

Mr. CARR. But you did ask me what this particular group was set up to do.

Mr. GLICKMAN. Yes.

Mr. CARR. And that is what this group was set up to do.

Mr. GLICKMAN. But aren't you set up to also deal with other kinds of national emergencies as well, other than full mobilization in the event of war?

Mr. CARR. I used that as an illustration of one of the scenarios that we would be dealing with, just one of them, but it's——

Mr. GLICKMAN. Yes?

Mr. CARR. It's within that context that the security issue would be dealt with.

At a given point in time, what does your information processing system have to do? Security is only one part of that total problem that has to be addressed.

Mr. GLICKMAN. Mr. Campbell, you had a comment there?

Mr. BRUCE CAMPBELL. To go back, sir, to your question and Frank's response, if we take off the hats that we're wearing sitting before the committee today, I have to go in my normal agency role to GSA for a delegation of procurement authority to acquire a computer system.

I crank in a number of these things since it is on our agency's—it's part of our agency director's requirement to make sure that the protection that is required to support the data that we have in our computer systems is adequately protected.

When we inherited what we inherited in 1981, we found that the computer system was old, archaic, and did not indeed do that.

We set about it, looking at the guidance that Mr. Carr's office puts out, the OMB directives, and, as the agency responsible, built those kind of things into our upgrade of our computer system, and we do have in the distributed systems that are in right now all those levels of protection, not just one level but from the physical, the exterior fences, the locks on the computer terminals themselves, the improved keyword and password process that we use, the cryption of the lines, et cetera, right on down the line, and that's an example of how an individual agency would indeed use the guidance that's on the books today.

Mr. GLICKMAN. Well, I just want to be—make sure that you're as concerned with protecting these computer systems from disruption as much as you are dealing with something happening after an emergency occurs.

You know, it's not so much of a fine line because we'd just as soon not have to deal with the emergency. I realize that you have to be prepared for it, but it just doesn't seem to be—the focus is not heightened enough in Government generally.

I'm not trying to put the blame on you. It's just the focus is not there on protecting those systems, and that's just—that's because we have become enamored technologically with new systems we're going crazy with developing, and we're just moving very fast technologically, and it may be impossible to protect those systems,

we're going so fast; and I just want to make sure somebody in Government is dealing with that.

Mr. CARR. I think you have to think about it as a multi-system process. There isn't one point of attack. We take one approach through the system planning itself.

Mr. Wright made reference to A-123. I think the A-123 mechanism that is being put in agencies, which addresses the operation of the organizational components to deal with the programs, to deal with administrative portions of it, tend to look at the vulnerabilities of data as part of that A-123 analysis.

That's going to give rise, I think, to a better statement of what the security requirements are of the system.

Mr. GLICKMAN. OK. Do you plan to broaden your activities—this group—perhaps in the area of protection of critical computer systems more directly than what you've done in the past?

Mr. BRUCE CAMPBELL. We feel that the overall guidance that we're trying to bring into focus for all the departments and agencies to use would indeed do that, so that we don't indeed have various and sundry levels of protection independent of the overall acquisition and the planning process.

I think Mr. Wright got into a little bit of that when he used the budget process as the vehicle, and the OMB data calls that are part of it, to focus, and we would hope that our product would feed into that.

Mr. CARR. If I could——

Mr. GLICKMAN. Sure.

Mr. CARR [continuing]. Expand on that, again, Mr. Wright made a particular point of the 5-year planning process—the improvements that are contemplated there.

The eventual intent of the planning process is to create a Governmentwide data base that will identify, again, not just the computer systems that exist in the Government but the application systems as well.

One part of that data base would identify for each of those application systems who the owner of that system is, and that's, again, the same point I was making earlier. You have to drop down to that level before you even begin to be able to talk to someone who truly understands what the system is to do, what the data contains, who are the people that have an interest in it, and what the essential characteristics are of that particular system.

So that 5-year planning process and that automated data base is going to give the kind of governmentwide information that is necessary to address the kind of issue that you're dealing with.

Mr. GLICKMAN. OK. We appreciate very much your testimony today.

[The prepared statements of Mr. Campbell and Mr. Carr follow:]

Joint Statement
Of
Bruce J. Campbell and Frank J. Carr
Co-Chairmen
of the
Automated Information Processing Task Force
Emergency Mobilization Preparedness Board
before the
Subcommittee on Transportation, Aviation and Materials
House Committee on Science and Technology
Hearings On
Computer and Communications Security and Privacy
U.S. House of Representatives

September 24, 1984

Mr. Chairman and Members of the Subcommittee:

I am Bruce Campbell, Assistant Associate Director for Information Resources Management within the Federal Emergency Management Agency.

My distinguished colleague, Mr. Frank Carr, is Assistant Administrator for Information Resources Management within the General Services Administration. We have been asked by Mr. Robert McFarlane, Assistant to the President for National Security Affairs, to represent the Emergency Mobilization Preparedness Board (EMPB) before this subcommittee today. We co-chair the task force on Automated Information Processing (AIP) for the Government Operations Working Group under this Board.

We appreciate the opportunity to speak to you today concerning a subject which is of vital importance to our nation's interest and more specifically, the survivability of our governmental processes. That is, computer and communications security and privacy.

The Emergency Mobilization Preparedness Board (EMPB) was established by President Reagan on December 17, 1981, to ensure that the government has the capability to provide for the security of the Nation and to protect its people, values and its social, economic, and political structure, and to ensure that government at all levels, in partnership with the private sector and the American people, can respond rapidly and effectively to any national security or major domestic emergency.

The Board is chaired by Mr. McFarlane, and consists of representatives of 23 key Federal departments, agencies and executive offices at the Deputy or Under Secretary level, normally meeting quarterly. The charter of the Board requires it to develop overall mobilization preparedness policy and a dynamic plan consistent with that policy to improve the nation's capability to respond to major domestic or national security emergencies. The Board has authority to resolve mobilization preparedness issues within the framework of current Administration policy.

The Board's policy formulation is carried out by working groups in thirteen functional areas, one of which is the Government Operations Working Group chaired by the Federal Emergency Management Agency. Their interest in the automated information processing (AIP) area began with activities initiated in the Emergency Communications Working Group, on which both Frank Carr and I sit as members. The problem was identified as an increasing reliance on AIP in support of both government and industrial operations. This increasing dependence renders the Government particularly vulnerable in the event AIP supporting national security or emergency preparedness functions is impaired or lost. Heretofore, there has not existed an integrated government program to mitigate the consequences of the loss of AIP supporting critical functions.

Adding to this problem of national security/emergency preparedness (NS/EP) vulnerability, there are unique considerations contributing to the Federal AIP problem. For example, computer and telecommunications equipment and systems in the Federal Government inventory may have been supplied by one thousand or more vendors, including some equipment which is obsolete by GSA standards. The Government has more than 16,000 computers in its current inventory, most of which are incompatible in terms of operational integration. Nobody at this time knows just how many application systems there are in the Federal Government. Further, it is difficult to achieve interagency agreement on what constitutes a "critical AIP system."

Further compounding the problem is the continuing and rapid proliferation of new information processing equipment and systems products such as word processors and personal computers. Also, many systems continue to be poorly documented, and successful operation of some systems depends on the interaction and knowledge of only a few key people. Besides the few key people who operate the AIP system and provide the information essential to decision-making in an emergency or disaster environment, there are many, many more who are intimately involved in the "care and feeding" of AIP. We refer to these resources as making up the AIP infrastructure.

The definition which the AIP Task Force has adopted for the term AIP is "the collection, storage, manipulation, presentation and distribution of data primarily by machines to provide information needed to support management decisions and operations." AIP resources include computer processors, systems and application programs, data bases and files, procedures, and human resources. AIP is a part of information resources management (IRM), which encompasses all automated and manual handling of data including computer processing and telecommunications.

The Emergency Communications Working Group (ECWG) reviewed the problem and proposed that the thrust of the Board effort should be to reduce the vulnerability of NS/EP functions resulting from the Nation's dependence upon AIP by carrying out Government and private sector planning in support of emergency operations instead of focusing on the security, survivability and endurance of resources used to support normal operations. They presented three alternatives to the full Board in May of 1983. These alternatives were:

1. Have Federal agencies address the AIP issue both with respect to their agency and to the private sector groups to whom they are principal Government liaison.

2. Assign action to an EMPB working group (existing or new) for development of an integrated EMPB approach which would then assign action to each working group for its respective functional area.

3. Recommend to the Cabinet Council For Management And Administration that a Presidential Initiative On AIP For Emergency Operations be established.

After briefings and considerable discussion of the alternatives by the Board members, a compromise was reached. The initiative would be retained at the Board with the Government Operations Working Group directed to establish a subworking group which would be co-chaired by Frank Carr (GSA) and myself representing FEMA. We would assemble the necessary expertise from interested agencies and work the problem while coordinating with the Reform 88 Project.

The AIP Task Force was formally established by the Government Operations Working Group at a meeting in March of 1984 at which time they adopted a workplan. Membership presently consists of principal representatives from nine Federal Agencies having essential emergency functions during a nationally declared emergency.

Our first assigned task which we are presently working is to develop guidance for Federal departments and agencies toward assisting them in developing their own plans for the use and protection of AIP in emergency situations.

When completed, this guidance will be distributed to all Federal agencies and departments in a Federal Preparedness Circular by FEMA's National Preparedness Programs Office of Mobilization Preparedness.

The AIP task force is also coordinating with an AIP task force in the private sector which was created by the National Security Telecommunications Advisory Committee to the President which was established in September 1982 under Executive Order 12382. This NSTAC AIP task force is made up of 11 major companies representing elements of the telecommunications industry. Their initial efforts were to identify and scope the issues critical to establishing a framework for joint Government/industry planning and toward improving the survivability of AIP capability which supports national telecommunications systems.

They identified three types of AIP to be addressed. These types are:

1. Embedded AIP collocated with, and in direct support of normal telecommunications functioning, characterized by system controllers and switching processors;

2. AIP that telecommunications operational support is dependent on for service or service restoration, such as data bases for configuration management and restoral activities;

3. AIP required to support all Government NS/EP functions in general.

This third category of AIP is the area being addressed by the EMPB AIP task force.

In the past, emergency preparedness efforts within both the private sector and the Federal Government have usually been identified principally with providing backup facilities in the event of equipment failure or loss of capability because of fire, floods, earthquakes and other emergencies, man-made or natural. They all assume a limited geographic problem area and are directed at achieving something approaching a "normal" level of operations.

Contingency planning for AIP is not simply a matter of identifying certain functions performed in peacetime as critical under emergency situations. It requires an understanding of how the emergency situation modifies the agency mission and the consequent decision support information required. While emergency communications seems to be an area for which some reasonable plans have been developed, AIP systems, because of their greater proliferation and complexity, will take much time and involve a great many more functional areas and people in both the private sector and the Federal Government.

As a concerted effort, we hope to achieve several significant goals in support of national security and emergency preparedness. These goals include:

1. Establishing an awareness within both private industry and the Federal Government of the criticality of certain AIP systems to essential emergency functions and operations during periods of crisis or major disasters.

2. Developing methodologies and procedures for identifying and assessing the vulnerabilities of AIP systems which support NS/EP functions.

3. Developing methods for identifying AIP deficiencies and requirements for AIP resources where the resources do not currently exist.

4. Establishing the framework for a survivable infrastructure architecture to support critical NS/EP AIP systems.

(By infrastructure, we mean the collection of basic resources such as facilities, equipment, services, and installations required to support AIP operations. These resources include such categories as energy including electric power and environmental systems, transportation for personnel, maintenance parts and services, communication lines and systems, personnel and the food, water and health services to support the personnel, civil security protection such as police and fire, and so forth. As you can see, describing the overall infrastructure to support NS/EP AIP can become extremely complex. Managing it effectively during a crisis will tax the Nation's capability for integrated planning to the highest degree.)

As you can see from the varied actions initiated with the participation of the Federal agencies and departments, and FEMA's mission responsibilities, we have been making significant progress toward improving the overall AIP posture of the Federal Government. Each planning step includes concise security considerations as part of the integral planning process. These actions are totally integrated with our program plans and requirements.

We believe these steps will contribute to ensuring that information resources are acquired, enhanced, utilized, disposed of, and protected in cost-effective ways while achieving FEMA's goals.

Mr. Chairman, Mr. Carr and I would like to thank you for this opportunity to present to this Subcommittee what we believe are significant steps toward improving computer and communication security in support of national security and emergency preparedness programs and functions. We would be pleased to respond to questions. Thank you.

Mr. GLICKMAN. Our next witness is Mr. Richard P. Kusserow, inspector general of the Department of Health and Human Services.

STATEMENT OF RICHARD P. KUSSEROW, INSPECTOR GENERAL, DEPARTMENT OF HEALTH AND HUMAN SERVICES, ACCOMPANIED BY JOHN I. MOLNAR, PROGRAM ANALYST, OFFICE OF PROGRAM INSPECTIONS

Mr. KUSSEROW. Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you, sir. Why don't you go ahead and proceed?

Mr. KUSSEROW. With your permission, I'd like to submit my full statement for the record——

Mr. GLICKMAN. Sure.

Mr. KUSSEROW [continuing]. And summarize, to allow maximum time for questioning.

Mr. GLICKMAN. Do you want to just tell the committee who is——

Mr. KUSSEROW [continuing]. Yes. Along with me today is Jack Molnar, who is from our Office of Program Inspections.

Mr. GLICKMAN. OK. Go ahead.

Mr. KUSSEROW. I would like to start out, if I may, Mr. Chairman, by thanking you for focusing on this critical issue of computer security, an area where there cannot be too much attention. Indeed, your reference to the veritable explosion of information that is taking place is a result of these computerized systems.

It's hard for us to contemplate the fact that more information is being collected, stored, manipulated, retrieved in our lifetime than in all other lifetimes of humanity, going back to that first caveman who emerged from a cavern in southern France leaving a pictorial history of a hunt.

As a result of that, we have learned to become very dependent upon these computerized systems. In fact, this Government could not fulfill many of its missions without them. In our department, we have 36 million Social Security checks being processed each month, which would be an impossible feat without automated data processing; and we have millions of medicare claims being reviewed, evaluated, and paid by the aid of computers.

For example, research in our department through the National Institutes of Health develops modern medical wonders through the use of advanced data processing techniques. The fact is that we are very, very heavily dependent upon these systems.

As was pointed out, there are over 20,000 mainframe systems. We certainly are looking forward to probably somewhere in the neighborhood of a half million micros and minis being in place by the end of the decade. So I don't think that anybody can deny that the computer is here, it's here to stay, and that it probably will become even more pervasive in the way we do business.

We, in the Federal Government, are witnessing a very traumatic event, and that's the virtual disappearance of all hard copy. It's especially hard for those of us in the inspector general community, who are investigators and auditors, to realize we won't have paper to work with.

But the crucial question as far as we're concerned in the inspector general community, as well as the Government as a whole, is whether this beast which has been let loose upon the land, can be tamed and made a beast of burden, or whether we're going to have a monster that's going to be pretty much in an adversary capacity with us.

You pointed out earlier that this is really a twin problem, and I would like to just echo that, if I may.

You pointed out that there's also a problem of insuring that there's appropriate data in the computerized systems—that we have, in fact, an integrity of the data within the system.

The other half of that—and I don't think you can separate it—is the fact that we must ensure that there's integrity in the computerized systems themselves. It is my view that the inspector general community should focus on a twin track of trying to ensure that only appropriate data's is the system, and that the system is designed and working the way it should.

We have done a lot of work at HHS developing programs that point out beneficiaries of our programs who, in fact, are obtaining those benefits with Social Security numbers that are nonexistent or have never been issued or identifying health providers who are double billing the system using different provider numbers.

There's a whole range of things that we can do to take out inappropriate data, to make sure that it is not in the system and, once it's taken out of the system, to lock the door to prevent it from being reintroduced.

As a result of this approach, I think that we can probably come to grips with the rising technology in terms making limited human resources work to maximum capacity.

In the last 3 years, we've been able to increase savings by about 400 percent, without any staff increases, and I think this is, in large measure, due to using systems to tame systems.

But the second effort is equally important, and that is to tame the computer with proper internal controls and audits to ensure the integrity of computerized systems. Many systems today are running without the proper controls having been designed and put into place. With many of the systems undergoing redesigning and upgrading, I think it has become very, very critical that we ensure on the front-end side that—that we're building in the computer, features as you pointed out with the previous testimony.

For example, we're upgrading the Social Security computer systems, which are terribly antiquated, at a cost of one-half billion dollars. In the contracts are provisions to ensure that there will be proper security and an electronic audit trail to replace the paper audit trail that we're dependent upon today.

I think it is our role in the inspector general community, as watchdogs, to look and make sure that contractors or civil service employees that are involved in systems design don't take shortcuts that would allow controls to be bypassed, and thereby create for the future additional problems as we've had in the past.

The other point I would like to make along this line is that whatever is done in computer security in the field, we cannot forget the fact that the primary responsibility in a computerized system is with the people who operate the system. They cannot be given any

kind of license to pass that responsibility on to somebody else. They must maintain responsibility for it because they are the people that operate the system.

We must ensure that agency managers in overseeing programs that use computerized systems, do audit the systems, do look and make sure that the controls are functioning, and that we in the inspector general community, using our auditors and investigators, follow up to make sure that it's being done. I think that in all these areas it has not been done nearly enough.

To really get on top of the problem requires a recognition of the vulnerabilities of today's computerized systems and the skills to address them. To a great extent, a lot of the progress in the last couple of years has been due to you and other Members of the Congress who have focused attention on this area. You have gotten agency heads to realize that in fact this is an area that needs to be addressed, and that failure to address it could result in a lot of very, very serious problems on a wide scale rather than in isolated circumstances, as has been the case to date.

As a result, a couple of years ago we realized that there had never been a definitive study in the Federal Government on computer security—and the fact of the matter is, there has been virtually nothing done in the private sector in terms of a definitive study. We felt it was high time that something be done to determine the extent to which our computerized systems in the Federal Government are vulnerable to fraud and abuse. The President's Council on Integrity and Efficiency formed a special computer security project to look governmentwide at the vulnerabilities of systems to fraud and abuse. I was asked to chair that project.

The resulting report which was published just a little over 1 year ago on the first phase, represented the first in-depth examination. It followed other formats that were similarly going on in the private sector, which I'll allude to in a moment. It provided us a lot of good insight, but in some respects it provided more questions than it did answers.

The study findings are based on analysis of 172 cases—69 of which were fraud, 103 abuse—that were identified by 12 agencies, and, in summary, the cases yielded the following information: first, that the scope of the problem still is unknown after we've done the study, because agencies do not systematically track computer-related fraud cases in their fraud tracking systems. Most agencies don't track abuse at all.

In part, as a result of this aspect of the report coming out, we had some changes made with the fraud and corruption tracking system in the Department of Justice. The Department of Justice had no way in which they could retrieve any information on cases that they had prosecuted that were computer fraud in nature.

As a result of the report, they developed data elements that would allow us now to go back and extract from the Department of Justice prosecutions related to computer fraud.

One of the major problems the Department of Justice has traditionally had, as have many of the traditional law enforcement agencies in dealing in this area, has been the accent and focus on the violation rather than the nature of the operation that was victimized as a result of the crime.

For example, if you went to the FBI with regard to computer fraud, they couldn't really pull those cases out. But if you asked them about cases involving interstate transportation of stolen property, you'd find a certain number of them that related to computer fraud or which involved computerized transactions across the State line.

The same thing was true for Secret Service, which has now begun to institute a system to be able to retrieve these cases; or the Postal Inspection Service, or any of the other agencies. Foremost, however, is the Department of Justice which now can pull out those cases that have been successfully prosecuted that are computer related.

The nature of the cases were interesting in that most frauds involved theft of cash or assets through input manipulation. It seems that the area which is the most easily curable is the area where you input the information, and this is the area where you have the biggest problem. So it seems that in this case an ounce of prevention can really effect a pound of cure.

Most abuse cases involved theft of computer time for outside business or entertainment and represented a very minor threat to the actual system itself.

For example, computer-related fraud losses ranged anywhere from no money being extracted out of the system to documented losses for prosecution of $177,383.

Now, it is our belief that this figure is grossly understated because of the nature of prosecutors and investigators. They will prove that which they feel is necessary to make their case in the court and don't really pursue much beyond that. So the full scope of the losses aren't really fully determined by that process.

Responses on losses in abuse cases were very scant.

With regard to detection, the interesting thing to note is that it was not the computer security specialists, or the auditors, or the investigators, or even the program managers who were the ones doing most of the detection of the fraud and abuse cases. We found that over half the frauds and two-thirds of the abuses were found by operating personnel—civil servants who found something that was inappropriate and tracked it down to surface the problem.

Right along with this was the very significant fact that more of the cases were found by accident than by any other means. Once again, it was not a control that surfaced the problem, but it was detected by accident. Again, the accident was discovered and pursued by a fellow employee who surfaced the problem.

On the issue of controls, we found that many of the respondents—and these were the people that were dealing with the problem that had already surfaced—either did not answer, or gave incomplete, or illogical responses to questions on controls in the victimized systems.

The prevalence of accidental detection, however, alarms us because of the implied weakness in controls. Theoretically, if you have a good system of controls, no individual could be able to complete a full transaction in a sensitive situation. Yet, if most of the people that were committing the crimes and the abuses were allowed to be able to do that, then in fact that basic control was not working.

Now, since the report was issued, we've had two other reports come out, and you will hear from the American Bar Association representative on their recently issued report. They, too, conclude that computer crime is very serious and a growing problem and that the law enforcement community needs more expertise to deal with the problem.

The other study was done by the American Institute of Certified Public Accountants, focusing on the banking and insurance industries, and their findings parallel ours so closely as to be uncanny. It indicates that the problems that exist in those industries parallel very strongly the problems that we have in the Federal Government.

As a result of the study, we made recommendations centering on two main areas. First, we felt that the IG staffs needed more training and awareness of the vulnerabilities of the computerized systems that they are supposed to be watchdogs over.

We also recommended increased scrutiny of internal controls in computer-based systems, particularly through the processes that we've heard so much about already this afternoon on OMB Circulars A-123 and A-71.

Since the report was issued, a number of initiatives and activities have occurred and are in process. First, we in the IG community have set up auditor and investigator training programs that will teach them both to use computerized systems—in this case micros—to find inappropriate data within systems, and also to detect the vulnerable areas and eliminate opportunities for fraud as well as systemic weaknesses.

A second followup initiative was a computer-security seminar for the inspectors general and the assistant secretaries for management, which I cohosted with Richard Shriver, who was at that time the Assistant Secretary at Treasury. The idea there was to provide people who were responsible on the management side of the system's problem to get together with the investigators and auditors in the inspector general community, to pool our resources to complement what we do rather than go at cross purposes. All of this is part of an effort to raise the level of awareness and concern for this very serious problem area.

Because the initial phase of the study did not give us answers about how and why computer fraud was so prevalent in the Government, we have begun to interview all the perpetrators.

We are in the midst of interviewing those that have been identified to date as well as cases identified subsequent to the report. It is still too early to give any hard findings, but we are seeing that when supervisors lack knowledge, interest, or time to know what is going on at the working level, the environment definitely is vulnerable to computer-related fraud and abuse. This made it possible for a lot of the people to have perpetrated the crime in the first place.

Mr. GLICKMAN. You mean you went to talk to the defendants in criminal cases?

Mr. KUSSEROW. Yes, sir, all the ones that have been identified in our study and some of those subsequent to our study.

Mr. GLICKMAN. And these were people who perpetrated crimes on the government or generally?

Mr. KUSSEROW. No; these are the people who had committed computer-related crimes against the U.S. Government, against our computerized systems.

Mr. GLICKMAN. How many did you talk to?

Mr. KUSSEROW. Well, to date, we have interviewed about 30, and we still probably have at least that many more to go.

Mr. GLICKMAN. And were most of the crimes perpetrated against your agency or——

Mr. KUSSEROW. No; this is across the entire Federal Government. These are all the cases that have been identified by all the agencies of the Federal Government relating to computer fraud.

Mr. GLICKMAN. And most of these people were insiders, employees of the Federal Government?

Mr. KUSSEROW. We had a combination of both. We had some outside people who manipulated the input process in order to commit the fraud. Others we found on the inside, such as a claims representative at Social Security in our department, or people that were involved in similar capacities with the Food Stamp Program in Agriculture. So we've got a cross range, and I would certainly appreciate an opportunity to submit that report at the earliest opportunity.

Mr. GLICKMAN. We would like to have that report very much, when you finish it.

Mr. KUSSEROW. Another interesting thing about those interviews, Mr. Chairman, is that we begin to see another pattern emerge from the interviews, and that is the fact that a large number of them had incentive awards.

Most of those that did have incentive awards, received them within 12 months prior to being found to engage in the crime in the first place. This brings into question whether or not the old thought about people who are Government employees who are not getting a fair shake are——

Mr. GLICKMAN. Wait a second. Who got the incentive awards?

Mr. KUSSEROW. We're saying that we are beginning to detect a pattern, that among those Government employees who were found to engage in computer fraud and who were subsequently convicted for it, we have found that a number of them had received incentive awards within 12 months prior to being detected as committing a crime against the U.S. Government.

One of the old precepts is that people are motivated to commit frauds or otherwise damage computerized systems because they were not getting due recognition for their work. We are beginning to see that maybe that precept is not entirely true, and it will be very interesting to see whether that pattern holds up. As I say, Mr. Chairman, as soon as we have that report, I'd like to submit it to you.

Another thing that we are working on is in the area of front-end ADP systems review. Our staff is leading an interagency effort across the entire Federal Government to improve audit involvement and effectiveness during the design, development, implementation, or major modification of automated information systems.

The notion that the auditor or the investigator should always come in after the fact and should not soil themselves in the design

phase because it might affect their independence later on to come in and challenge it, is nonsense.

I think that this is such an important area that we must involve ourselves on the front-end side using our frame of reference, our perspective, as we're doing at Social Security—to make sure that there are not shortcuts being taken that would inhibit the development of proper controls in the system against fraud.

We are also developing as products of this project, an audit approach to looking at computerized systems that can be a model for all of the departments' inspectors general to follow, a documentation guide as to what to look for in the system to ensure the fact that controls are in place, and explanations of the roles and responsibilities of key players during a system's life cycle. We think that this will be particularly useful for both the program managers and for those that have to review the system from the outside. On all of the projects and efforts that we're working on, we will be delighted to submit these reports to the subcommittee as they are developed.

Now, Mr. Chairman, that concludes my summary remarks. I'll be happy to answer any questions that you may have for me at this time.

Mr. GLICKMAN. I want to thank you for excellent testimony, and we—some of the specifics in your report are things that go to the heart of the problem, what we're talking about, and things that we will try to improve, if we can, either through the regulatory process that Mr. Wright talked about, but I don't think that's going to be enough; I think it's going to take some Federal legislative action to push computer training, security training, and the awareness thereof using existing mechanisms.

But what—you know, I go back to page 5 of your statement. You state, "One overriding finding of this study is that we still do not know the scope of computer-related fraud and abuse in government." But would it be a fair—how would you characterize what you do know? Extensive? fairly extensive? serious?

Mr. KUSSEROW. I would say it's very serious. Any time that we have the kind of vulnerability that exists in our programs, it is serious.

One of the things that the recent prominence of hackers brought to light is that people who operate computerized systems thought that systems dealing with nonsensitive material didn't need to have the proper controls. So, therefore, they drifted into using systems that were extremely user-friendly—where you can talk to them in English and tell them what to do—and, as a result of that, invited amateurs on the outside to easily get into those data bases to do potential harm. People just didn't think that anybody would go through any kind of an effort, for example, to dial into a hospital computer system to get a patient's record.

We now know that you can't count on that any more, and that you have mischiefmakers that'll go into any system. We've got the technology available to innoculate our systems against most of the kinds of problems that we have been confronted with.

The issue is to get that technology to prevent and remove the systemic weaknesses that give rise to these fraud and abuse problems.

The technology is there. All you have to do is have the will, and you can take care of probably 99 percent of the problem—a very, very simple effort.

Mr. GLICKMAN. The will in your agency, HHS—I mean you manage billions and billions of dollars in payments in medicaid, medicare, Social Security. What are you doing in your department, in your agency?

Mr. KUSSEROW. Well you're quite right. We represent the largest agency in the Government. The fact is, our agency by itself matches that of any government in the world except the United States and the Soviet Union. We have about $300 billion in outlays.

The range of how good we are in terms of protecting our systems from pollution of inappropriate data being introduced into the system, as well as from people improperly accessing and manipulating the data, is from very spotty to quite good.

We have some of the worst computerized systems in the country. Social Security is a good example of that. We have five or six different systems, each built upon the other, that were designed a full score years ago, with people that used the most exotic formats and variations of it—probably to ensure their own longevity on the contract or in government. When they left or died off, there was nobody that understood the system. So we always had the manual override, which means that today, we have a very serious problem of not having an electronic audit trail to determine what people are doing with the system.

That is the reason why Social Security in 1981 proceeded to upgrade the system and move to a different system that would have the kinds of controls and audit trails to prevent that kind of problem from recurring.

As I pointed out earlier in my testimony, it's very important that I watch that process very carefully, because I believe, as you correctly pointed out in the previous testimony that you can't always be sure that just because it's in the RFP, that it gets the proper attention and that people won't take shortcuts.

Somebody has to make sure that those shortcuts aren't taken. In our department, I consider that I play a role in that process. We have an ADP audit division, the first in the IG community, and that is their main mission.

While we have poor systems, we also have some very good ones. We have some of the best computerized systems in the Federal Government, or, for that matter, in this land, at the National Institutes of Health, where they engage in very sophisticated health research. There, the sensitivity and integrity of that data, which is vital to research, is protected in the system. Therefore, you would find it very, very difficult to find weaknesses to abuse or defraud. So we have the full range.

I think across the Government we can generalize by saying that in those areas where there is an inherent security factor, there has always been an awareness of security. In national security particularly, thre is a much better record.

So in the Department of Defense and in the Department of Energy, they put a lot of effort into computer security. But even in those agencies, it could be spotty, could have weaknesses, especially where you found that they felt that the data was not really sensi-

tive or not of a national security nature. Once again, the hackers have shown that you can't take that assumption and ride with it without finding that you're going to be wrong.

So I think that there's an awful lot of work done in this area. I think that we've made surprising progress. I think it has taken a lot to do that. I think that we can make a lot more progress, and I think that there is no way we can let up in this area.

Mr. GLICKMAN. The audit trail problems that you said existed within Social Security, have they improved since there have been upgrading of computers since 1981 in that system?

Mr. KUSSEROW. Well, they are not on line yet, but they have made some basic improvements.

There are other things that we have done on site with the existing system to improve. We just didn't think that we should wait the 5 years that the redesign would take.

We felt that we must deal with the existing system to improve the security of that, and we've been doing that. We've been doing security inspections, we've been working with management, with the Social Security Administration, to tighten up the security procedures at all of the 1,300 district offices of Social Security and the six payment centers.

So we're making progress there in the short term with the existing systems while, at the same time, we're involving ourselves in the design of the new system, so that we just don't replicate the problems of the past into the future.

Mr. GLICKMAN. Do you have specific training—computer security training programs at HHS or——

Mr. KUSSEROW. Yes.

Mr. GLICKMAN. You do?

Mr. KUSSEROW. Yes, sir.

Mr. GLICKMAN. Are you—is the inspector general's office the one in charge of those programs?

Mr. KUSSEROW. Well, we have our own training program of course. We also use contractors to provide specialized training, and in addition to that, the Assistant Secretary for Management and Budget has specialized training programs in the area of computer security. We have been fostering in the various components in the department that management set up computer security training programs. If there is any one point that I would like to leave with you, Mr. Chairman, it is the sense that I don't believe anybody should be let off the hook in the area of computer security. The person who is using the system and operating the system has the primary responsibility for the security of that system, and that no outside agency should be asked to assume that.

There are just too many systems being developed. We must hold the people who operate those systems accountable and keep as close as we can to the people that are operating the system.

Mr. GLICKMAN. Well, you know, I've the strong impression from your testimony as well as others that—that perhaps Federal Government computer auditors don't have the controls that they need to deter or prevent computer crime from occurring.

You've talked about the problems in the Social Security system. If you had to recommend a couple of things that ought to be done in the Federal Government, what would they be? More forceful

leadership by OMB? more extensive training programs in the Federal system? what?

Mr. KUSSEROW. I think—I think all of it.

I think that primarily, you should recognize that 90-some-odd percent of the problem is in the area that is the most easily curable. The whole input process is where we have the greatest vulnerability. It is the easiest area to build controls in.

If we were to focus just on the simplest control features in the computerized system, we would eliminate nine-tenths of the problem. Then we could turn around and focus in on the more sophisticated types of vulnerabilities.

So, I would say the number one thing is—is doing exactly what you're doing here today and have been doing in the past, and that is focusing the attention of the American people on this problem and putting pressure on the Federal Government not to lose momentum, to keep moving toward dealing with this problem.

We've just got too many people. We've got hundreds of thousands of people in the Federal Government that are involved in these systems. We must make sure that everybody involved in it gets his feet wet and goes to work against it. I think the biggest area and the biggest success that we can have is in the area of raising awareness and accountability of people who operate the system.

I'd like to go back to the extent of how big you think the computer fraud and abuse problem is in government. Let's start with your agency. Do you have any estimates on total dollar involvement, total number of times that computers have been improperly accessed, inputted, invaded?

Mr. KUSSEROW. Mr. Chairman, I can give you all the reported incidents in the Federal Government, which is part of our report, and, if you like, I can submit that for the record.

[The information is available in committee files:]

Mr. KUSSEROW. But as far as the amount of fraud and abuse that exists, it's almost impossible to make estimates.

Some years ago, a predecessor of mine at HHS made an estimate as to the amount of fraud and abuse they thought was in the then HEW. There was quite a tumultuous response from the American people and the Congress over that. Yet in the time since then, we have provided more savings than was in that original report. I'm here to tell you that we're not through. There's still probably a role for the inspector general at HHS to root out some more fraud and abuse.

So, I will say that it's not probably pervasive, but the problem that would give rise to opportunities may approach that, and I think we're fortunate. We're fortunate we haven't had more problems in this area, and more should be said about what could happen than what has happened.

What has happened has been relatively small against what could happen in the future, and that's where our accent should be.

So, I can't tell you how much. I can tell you that I don't feel comfortable about the vulnerabilities as they exist now.

Mr. GLICKMAN. Do you think there is a need for a more formalized or centralized way to train Government computer people about security and to assist agencies in implementing controls?

Mr. KUSSEROW. One of the problems that we have had, as in the projects that I've been associated with on the President's Council on Integrity and Efficiency, has been to deal with agencies that are so dissimilar in nature.

Some agencies are regulatory in nature, some are procurement-oriented agencies, some are benefit-oriented agencies, and they have different systems; they have different levels of concern.

For example, when you talk about computer security maybe at the Department of Energy or Department of Defense, you're talking about, ensuring proper encryption, line security, and things like that.

In other agencies and many parts of our department, for example, I'm just concerned about people that scotch-tape their access numbers on the terminal so they won't forget them, so that anybody else can come along and use them.

So, you're really talking about apples and oranges and peaches and pears.

So, I don't think any single program will do it, but we must have agency managers look at their own system and respond to the requirements of A-123 and A-71 to point out where the vulnerabilities are and then design a package of controls for that. Similarly, those people that are responsible for auditing those systems should have the specialized training to deal with the kinds of security problems that exist with the system in question.

So, to answer your question in summary, I would say that it depends upon the system, and each system is different and requires different skills. But, 90 percent of the problem can be cured by some very baseline security measures, and we could look at those. That is, what are the security features that are common to all systems, and concentrate on those, and I think we'd get most of the problems just by doing that.

So from that standpoint, yes; as far as the specialized nature of the systems, no.

Mr. GLICKMAN. Let me just go to a specific case in terms of this audit trail. All Members of Congress are faced with problems from constituents who have, let's say, problems with the Social Security System on improper categorization of benefit data, and there was a story in "U.S.A. Today" last week; I don't know if you saw it; but there has been—the story said that there has been underpayments in many cases of several billions of dollars, not by fraud or deceit but by time delays and inputting data as well as improper data that's actually been put in there.

I guess what worries me after listening to you is, let's say specifically in the Social Security System is—is that even if there are mistakes made in inputting, that it may be impossible for anybody to find out about them or correct them once they're made.

Mr. KUSSEROW. That's exactly right. But I will say this, Mr. Chairman, that we are working very hard on that. We started out on my testimony by acknowledging your great concern in this area and the concern that I share with you. That is, we can't talk about computer security, the security of computerized systems, the integrity of computerized systems, without talking about the data within the systems to assure that the data is appropriate, and that the system itself that maintains the data has integrity. To do that,

we need much more in the way of front-end controls, prepayment screens, and edits that would question things that appear inappropriate on their face while the person is still standing there or while the document is still there. So, in this way, the data doesn't get into the system and pollute that database, and then later on compound the problem of trying to find it.

So, the whole thrust of what we're doing in that area in the President's Council on Integrity and Efficiency is focusing on what it is that we can do to put front-end controls on the system that would identify inappropriate data that's being entered into the system. It is far easier to keep it out of the system than it is to go and find it after it is in the system. That is a very great responsibility and perhaps as important as the other aspect of ensuring that the systems themselves are—are secure.

Mr. GLICKMAN. Mr. Kusserow, we want to thank you for your testimony today; it's been excellent. I would appreciate your supplying the committee with the data that you mentioned in your—in your testimony, and also if we work on legislation, I would like to have the opportunity of talking with you or your people in greater detail to try to maybe determine what, if anything, the Congress can be doing to improve sensitivity to this issue.

Mr. KUSSEROW. Thank you, Mr. Chairman. I'll be delighted to supply whatever resources we can.

Mr. GLICKMAN. OK. Thank you very much.

[The prepared statement of Mr. Kusserow follows:]

STATEMENT OF

RICHARD P. KUSSEROW

INSPECTOR GENERAL

DEPARTMENT OF HEALTH AND HUMAN SERVICES

BEFORE

SUBCOMMITTEE ON TRANSPORTATION,

AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 24, 1984

MR. CHAIRMAN, THANK YOU FOR THE OPPORTUNITY TO TESTIFY BEFORE THE SUBCOMMITTEE TODAY ON THE PROBLEMS OF COMPUTER AND COMMUNICATIONS SECURITY. YOU REQUESTED THAT I DISCUSS THE WORK OF THE COMPUTER SECURITY TASK FORCE WHICH I CHAIR FOR THE PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY (PCIE) AND PRESENT OUR ACCOMPLISHMENTS TO DATE AND ANY PRELIMINARY RESULTS WE CAN DISCUSS FROM WORK IN PROGRESS.

TODAY WE ARE IN THE MIDST OF AN INFORMATION EXPLOSION. MORE INFORMATION WILL BE COLLECTED, STORED, MANIPULATED AND RETRIEVED IN OUR LIFETIME THAN IN ALL THE PREVIOUS GENERATIONS PUT TOGETHER.

THE ENTIRE FEDERAL GOVERNMENT IS HEAVILY DEPENDENT ON COMPUTERS FOR PRACTICALLY EVERY FACET OF ITS DAILY ACTIVITIES. OVER 20,000 MAIN FRAME COMPUTERIZED SYSTEMS HAVE BEEN IDENTIFIED TO DATE, WITH ADDITIONAL ONES BEING ADDED ALMOST DAILY. BY 1990, WE WILL HAVE OVER A HALF MILLION MICROCOMPUTERS IN PLACE. WITH THIS WE ARE WITNESSING THE VIRTUAL DISAPPEARANCE OF HARDCOPY. THIS IS ESPECIALLY CRITICAL FOR THE GOVERNMENT AUDITOR AND INVESTIGATOR WHO ARE USED TO PAPER AUDIT TRAILS.

THE CRUCIAL QUESTION FOR THE INSPECTOR GENERAL COMMUNITY, AS WELL AS FOR THE GOVERNMENT AS A WHOLE, IS WHETHER COMPUTERS WILL SERVE US OR OVERWHELM US. INSPECTORS GENERAL CAN MAKE COMPUTERS SERVE US IN TWO WAYS. FIRST, WE CAN USE COMPUTERS TO TAME

COMPUTERS BY USING THE COMPUTER AS AN AUDIT OR INVESTIGATIVE TOOL TO SEARCH FOR DATA THAT IS INAPPROPRIATE OR ILLOGICAL.

SECOND, WE MUST AUDIT THE COMPUTERIZED SYSTEMS THEMSELVES AND INSURE THAT THE PROPER INTERNAL CONTROLS ARE BEING BUILT INTO THE MANY NEW SYSTEMS DESIGNS THAT ARE UNDERWAY TODAY. COMPUTER SECURITY IS PRIMARILY AN AGENCY RESPONSIBILITY. AGENCY MANAGERS MUST IMPLEMENT COMPUTER SECURITY POLICIES AND PRACTICES, AND INTERNAL AUDITORS AND INVESTIGATORS MUST AUDIT THE CONTROLS OR INVESTIGATE ABUSES OF THOSE SYSTEMS. TO DO THIS, HOWEVER, WE NEED A THOROUGH KNOWLEDGE OF THE VULNERABILITIES OF THE CURRENT COMPUTER SYSTEMS AND THE SKILLS TO ADDRESS THEM.

PCIE Study of Computer-Related Fraud and Abuse in Government Agencies

THE PCIE WAS CONCERNED ABOUT THE NEED TO UPGRADE THE AUDIT AND INVESTIGATIVE SKILLS AND COMPUTER SECURITY ACTIVITY WITHIN THE IG COMMUNITY IN VIEW OF THIS AUTOMATION EXPLOSION IN GOVERNMENT. AS A RESULT, THE COUNCIL CHARGED ME TO LEAD THE COMPUTER SECURITY PROJECT TO PROVIDE THEM WITH A PERSPECTIVE ON THE NATURE AND SCOPE OF COMPUTER-RELATED FRAUD AND ABUSE IN GOVERNMENT AGENCIES. SPECIFICALLY, THE COUNCIL WANTED TO KNOW:

- IS COMPUTER-RELATED FRAUD AND ABUSE A PROBLEM IN GOVERNMENT?

- o If so, what are the characteristics?

- o What should the Inspector General community do to detect and prevent future occurrences?

- o What additional computer security expertise and activity are required in the Inspector General environment?

The Task Force I convened to study the problem included experts in computer security, computer auditing, statistical analysis, and management/program analysis from the Departments of Agriculture, Commerce, Defense, and Treasury; the National Aeronautics and Space Administration; and the General Accounting Office.

Because of the lack of any reliable data on the size or extent of the problem, let alone the causes, we decided to survey the Federal agencies to compile and analyze the reported cases of computer-related fraud and abuse. This survey became the first comprehensive study of the problem in the Federal Government.

To accomplish this, we directed survey questionnaires to the Agencies through the Inspectors General and to the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and the

CHIEF POSTAL INSPECTOR TO OBTAIN DATA ON CASES DISCOVERED BETWEEN JANUARY 1, 1978 AND MARCH 31, 1982.

TO OBTAIN THE BROADEST POSSIBLE DATA BASE AND ANALYZE THE DIFFERENCES BETWEEN SUBSETS OF CASES, WE INCLUDED BOTH FRAUD AND ABUSE IN THE SURVEY. ALTHOUGH DEFINITIONS ARE OFTEN HOTLY DEBATED IN THIS AREA, WE ADOPTED, FOR ANALYSIS PURPOSES, THE FOLLOWING DEFINITIONS:

> COMPUTER-RELATED FRAUD INVOLVED AN ILLEGAL, INTENTIONAL ACT DESIGNED TO DECEIVE OR MISREPRESENT IN ORDER TO OBTAIN SOMETHING OF VALUE. THE COMPUTER MUST HAVE BEEN USED TO PERPETRATE OR COVER-UP THE ACT.
>
> COMPUTER-RELATED ABUSE INVOLVED THE MISUSE, DESTRUCTION, ALTERATION, OR DISRUPTION OF DATA PROCESSING RESOURCES. ALTHOUGH THE ABUSE IS INTENTIONAL AND IMPROPER, IT DOES NOT NECESSARILY IMPLY VIOLATION OF A SPECIFIC LAW OR THE PRESENCE OF MISREPRESENTATION.

CONSEQUENTLY, THEFT OF COMPUTER TIME, WHICH IS SOMETIMES CATEGORIZED AS FRAUD (AND WOULD BE UNDER PENDING LEGISLATION), WAS INCLUDED AS ABUSE FOR OUR PURPOSES.

FINDINGS

ONE OVERRIDING FINDING OF THIS STUDY IS THAT WE STILL DO NOT KNOW THE SCOPE OF COMPUTER-RELATED FRAUD AND ABUSE IN GOVERNMENT. AGENCIES DO NOT SYSTEMATICALLY DISTINGUISH COMPUTER-RELATED FRAUD CASES FROM OTHER TYPES OF WHITE-COLLAR CRIME IN THEIR CASE TRACKING SYSTEMS. MOREOVER, MOST AGENCIES DO NOT HAVE ANY TRACKING SYSTEM AT ALL FOR ABUSE CASES. CONSEQUENTLY, WE HAD TO RELY ON INDIVIDUAL MEMORY OR AD HOC RECORDS WHICH SOME AGENCIES DID KEEP. IN ADDITION, NEITHER THE FBI NOR SECRET SERVICE WAS ABLE TO RESPOND BECAUSE AT THE TIME OF THE SURVEY THEY MAINTAINED THEIR FILE SYSTEMS BASED ON THE FEDERAL CRIMINAL VIOLATIONS UNDER INVESTIGATION AND THEREFORE DID NOT SPECIFICALLY IDENTIFY FRAUD OR LARCENY INVOLVING A COMPUTER.

IN RESPONSE TO OUR SUGGESTIONS AND CONCERN, HOWEVER, THE JUSTICE DEPARTMENT ADDED A UNIQUE IDENTIFIER TO ITS FRAUD AND CORRUPTION TRACKING SYSTEM (FACTS) FOR ANY COMPUTER-ASSISTED FRAUD CASES FORWARDED BY INSPECTORS GENERAL TO THE FBI OR TO THE U.S. ATTORNEYS. THE SECRET SERVICE ALSO REPLIED THAT IT WOULD TAKE STEPS TO INSURE THAT ITS MANAGEMENT INFORMATION SYSTEM WOULD INCLUDE IDENTIFICATION OF COMPUTER-RELATED CASES.

DESPITE THE PROBLEMS WITH DATA COLLECTION, 12 OF THE 22 AGENCIES WE SURVEYED (IN WRITING WITH PERSONAL FOLLOWUP) DID RESPOND WITH

A TOTAL OF 172 CASES WHICH MET OUR DEFINITIONS. OF THESE, 69 WERE CATEGORIZED AS FRAUD, AND 103 WERE ABUSE.

THE 69 FRAUD CASE CONSISTED PRIMARILY (93%) OF THEFT OF CASH OR DIVERSION OF ASSETS THROUGH INPUT MANIPULATION OF BENEFIT OR PAYROLL SYSTEMS. FOR EXAMPLE, ONE FEDERAL EMPLOYEE STOLE MORE THAN $100,000 BY REACTIVATING RECORDS FOR DECEASED BENEFICIARIES AND BY INTRODUCING FICTITIOUS RECORDS FOR NONEXISTENT BENEFICIARIES THROUGH HIS AGENCY'S COMPUTER INPUT PROCESS.

MOST (57%) OF THE 103 ABUSE CASES INVOLVED THEFT OF COMPUTER TIME FOR OUTSIDE BUSINESSES OR ENTERTAINMENT. FOR EXAMPLE, ANOTHER FEDERAL EMPLOYEE KEPT THE RECORDS OF HIS OUTSIDE CONSULTING BUSINESS ON HIS AGENCY'S COMPUTER, USING THE SYSTEM TO KEEP ACCOUNTS RECEIVABLE AND MAILING LISTS AND TRANSMIT MESSAGES TO HIS CLIENTS.

THREE-FOURTHS OF THE PERPETRATORS OF EITHER FRAUD OR ABUSE CASES ACTED ALONE. THIS FINDING IMPLIES THAT COLLUSION WAS NOT NECESSARY BECAUSE THE BASIC MANAGEMENT AND ACCOUNTING CONTROL OF SEPARATION OF DUTIES WAS NOT PRESENT.

MOST OF THE PERPETRATORS OF EITHER FRAUD OR ABUSE WERE NON-SUPERVISORY, FEDERAL EMPLOYEES. THE DIFFERENCES BETWEEN FRAUD AND ABUSE PERPETRATORS WAS EVIDENT, HOWEVER, IN THE

CHARACTERISTICS OF SALARY LEVEL AND JOB AREA. FOUR OUT OF FIVE OF THE FRAUD PERPETRATORS EARNED $20,000/YEAR OR LESS, WHILE HALF OF THE ABUSE PERPETRATORS EARNED OVER $20,000/YEAR. MOST OF THE FRAUD PERPETRATORS (62%) WERE FUNCTIONAL USERS OF THE COMPUTER SYSTEMS, WHILE AN ALMOST EQUAL PERCENTAGE (59%) OF ABUSE PERPETRATORS WERE DATA PROCESSING PERSONNEL.

MOST OF THE PERPETRATORS, WHETHER OF FRAUD OR ABUSE, WERE SANCTIONED BY EITHER JUDICIAL OR ADMINISTRATIVE ACTION. ONLY 16 PERCENT OF THE FRAUD PERPETRATORS AND 30 PERCENT OF THE ABUSE PERPETRATORS HAD NO ACTION TAKEN AGAINST THEM. ALMOST THREE-FOURTHS OF THE FRAUD PERPETRATORS WERE THE SUBJECTS OF SOME TYPE OF JUDICIAL ACTION, WHILE OVER THREE-FIFTHS OF THE ABUSE PERPETRATORS WERE THE SUBJECTS OF ADMINISTRATIVE ACTION ONLY.

WE ASKED RESPONDENTS TO PROVIDE AMOUNTS OF LOSS FOR BOTH FRAUD AND ABUSE CASES. WE RECEIVED LOSS DATA IN 65 OF THE 69 FRAUD CASES, WITH RESPONSES RANGING FROM $0 TO $177,383. THE HIGHEST INCIDENCE OF LOSS WAS IN THE RANGE FROM $10,000 TO $100,000, AND ONLY EIGHT PERCENT OF THE FRAUD CASES HAD LOSSES OF OVER $100,000.

WE CONCLUDED, HOWEVER, THAT THE LOSSES IN A SIGNIFICANT NUMBER OF THESE CASES WERE UNDERSTATED. THE QUESTIONNAIRE ASKED RESPONDENTS WHETHER THEY FELT ACTUAL LOSSES WERE HIGHER THAN THE

FIGURES THEY GAVE US. ALMOST HALF (48%) OF THE RESPONDENTS ANSWERED "YES". THIS RESPONSE IS CONSISTENT WITH THE SYSTEMATIC BIAS FOUND IN MOST WHITE-COLLAR CRIME CASES. INVESTIGATORS USUALLY UNCOVER ONLY AS MUCH EVIDENCE AS THEY NEED FOR A GOOD PROSECUTION.

FOR EXAMPLE, A CLAIMS TECHNICIAN IN A FEDERAL BENEFIT SYSTEM CREATED FICTITIOUS BENEFICIARIES TO OBTAIN BENEFIT PAYMENTS FOR HER CO-CONSPIRATORS. ALTHOUGH THE EVIDENCE USED FOR PROSECUTION ESTABLISHED THE LOSS AS $102,000, INVESTIGATORS BELIEVE THE PERPETRATOR MAY HAVE ACTUALLY DIVERTED AS MUCH AS HALF A MILLION DOLLARS IN FRAUDULENT BENEFIT PAYMENTS.

RESPONSES ON LOSSES IN ABUSE CASES WERE VERY SCANT, WITH ONLY 33 PERCENT OF THE RESPONDENTS PROVIDING DATA. THESE FEW RESPONSES RANGED FROM $0 TO $5,214.

THE SURVEY QUESTIONNAIRE ASKED RESPONDENTS TO IDENTIFY WHO DETECTED THE CASES OF COMPUTER-RELATED FRAUD AND ABUSE AND HOW THE DETECTION WAS TRIGGERED. FOR ANALYSIS PURPOSES, WE GROUPED THE RESPONSES ON WHO DETECTED THE CASES INTO THREE CATEGORIES: (1) <u>OPERATING PERSONNEL</u>, INCLUDING MANAGERS, CO-WORKERS AND DATA PROCESSING PERSONNEL; (2) <u>OVERSIGHT STAFF</u>, INCLUDING

AUDITORS, COMPUTER SECURITY OFFICERS, AND PROGRAM EVALUATORS; AND (3) OTHER, INCLUDING RECIPIENTS, CONTRACTORS OR VENDORS, AND LAW ENFORCEMENT OFFICERS.

WE FOUND THAT OPERATING PERSONNEL FOUND TWO TO THREE TIMES AS MANY CASES OF COMPUTER-RELATED FRAUD AND ABUSE AS EITHER OF THE OTHER TWO GROUPS. WITHIN OPERATING PERSONNEL, CO-WORKERS AND MANAGERS FOUND EQUAL AMOUNTS OF FRAUD. CO-WORKERS, HOWEVER, FOUND TWICE AS MANY ABUSE CASES AS DID MANAGERS.

FOR ANALYSIS PURPOSES, WE GROUPED THE RESPONSES WE RECEIVED ON FACTORS WHICH TRIGGERED DETECTION INTO THREE CATEGORIES: (1) ACCIDENT, WHICH INCLUDED CHANCE OCCURRENCE, CURIOSITY, AND REVENGE; (2) AUDIT, WHICH INCLUDED ROUTINE AND NON-ROUTINE AUDITS, AS WELL AS COMPUTER SECURITY REVIEWS; AND (3) CONTROLS WHICH INCLUDED MANAGEMENT REPORTS AND REVIEWS, NONCOMPLIANCE WITH PROCEDURES, AND OTHER INTERNAL CONTROLS.

WE FOUND THAT ABOUT HALF OF THE CASES OF BOTH FRAUD AND ABUSE WERE DISCOVERED BY ACCIDENT. THIS IS TWICE THE INCIDENCE OF DISCOVERY THROUGH EITHER OF THE OTHER TWO CATEGORIES.

FOR EXAMPLE, A FEDERAL EMPLOYEE FRAUDULENTLY OBTAINED OVER $104,000 IN A 1 1/2 YEAR PERIOD BY MANIPULATING INPUT TO SEND

FEDERAL BENEFIT CHECKS TO HIS OWN DIRECT DEPOSIT BANK ACCOUNTS. HE WAS DETECTED ONLY WHEN AN ALERT BANK CLERK HAPPENED TO NOTICE THAT THIS PERSON HAD OPENED SEVERAL DIRECT DEPOSIT ACCOUNTS AT THE SAME BANK IN DIFFERENT NAMES.

THE FINDING THAT MORE CASES ARE FOUND BY ACCIDENT THAN BY ANY OTHER MEANS IS ALARMING BECAUSE IT IMPLIES THAT FEDERAL AGENCY COMPUTER SYSTEMS HAVE EITHER INADEQUATE CONTROLS OR NONE AT ALL. THE FINDING ALSO POINTS TO A GREAT POTENTIAL FOR UNDETECTED FRAUD AND ABUSE.

WE ATTEMPTED TO GET MORE INFORMATION ON THE CONTROLS IN VICTIMIZED SYSTEMS THROUGH A SERIES OF SPECIFIC QUESTIONS ON WHICH TYPES OF CONTROLS WERE IN PLACE AND USED, IN PLACE AND NOT USED, IN PLACE AND OVERRIDDEN, OR NOT IN PLACE. THE RESPONSE RATE AND QUALITY, HOWEVER, WERE VERY POOR. ONE-FIFTH OF THE RESPONDENTS DID NOT ANSWER ANY OF THE QUESTIONS AND OTHERS OFTEN PROVIDED ILLOGICAL OR INCOMPLETE RESPONSES. IN ADDITION, OVER THREE-FOURTHS OF THE RESPONDENTS WERE UNABLE TO ANSWER WHETHER THE SYSTEM HAD EVER BEEN AUDITED, AND OVER TWO-THIRDS DID NOT KNOW WHETHER VULNERABILITY OR RISK ASSESSMENT PROGRAMS WERE IN PLACE.

Comparisons with other Studies

It is interesting to compare and contrast our findings with two recent reports--those of the American Institute of Certified Public Accountants (AICPA) and the American Bar Association (ABA), the latter which will also be presented in this hearing. Charts comparing these studies to our findings are appended to this statement.

The AICPA published its report in April 1984 on "The Study of EDP-Related Fraud in the Banking and Insurance Industries." This study, which began in 1978, served as a model to our PCIE study; in fact, we patterned our survey questionnaire after the AICPA survey instrument. The AICPA report of 119 fraud cases (85 banking and 34 insurance) shows interesting, and sometimes striking, similapities to the PCIE study:

- Perpetrators - In both reports, the primary objective or motive for the frauds was financial gain. Almost the same ratio (3 to 1) of nonsupervisory to supervisory employees were involved in EDP-related frauds in both reports. Of even more interest is predominance of users, rather than data processing personnel, in frauds. In the AICPA study cases, over 80 percent (as opposed to 62% in the PCIE study) of the perpetrators were users who

COMMITTED FRAUDS INVOLVING UNAUTHORIZED FILE CHANGES AND TRANSACTION MANIPULATION. SINCE THE AICPA DID NOT STUDY WHAT WE CATEGORIZED AS ABUSE, WE CANNOT SPECULATE IF A SIMILAR INVOLVEMENT OF DATA PROCESSING PERSONNEL IS PRESENT IN COMPUTER-RELATED ABUSE IN THESE INDUSTRIES.

- o Losses - ALTHOUGH THE AICPA REPORTED LOSS DATA IN SLIGHTLY DIFFERENT CATEGORIES, THE REPORTED CASES WITH LOSSES UNDER $100,000 ARE THE MAJORITY, AS WITH THE PCIE CASES. IT IS INTERESTING TO NOTE, HOWEVER, A HIGHER PERCENTAGE OF CASES OVER $100,000--14 PERCENT IN BANKING CASES AND 21 PERCENT IN INSURANCE CASES--THAN THE 8 PERCENT WE FOUND IN THE PCIE CASES. APPARENTLY, THE AICPA DID NOT INVESTIGATE WHETHER THESE LOSSES WERE UNDERSTATED. I WOULD VENTURE THAT THE SAME SYSTEMATIC BIAS TOWARD UNDERSTATED LOSSES THAT WE FIND IN WHITE-COLLAR CRIMES WOULD BE PRESENT HERE.

- o Detection - SIMILAR TO THE PCIE CASES, THE AICPA FOUND THAT OPERATING STAFF DISCOVERED OVER HALF OF THE EDP-RELATED FRAUDS (51% IN BANKING; 68% IN INSURANCE CASES). THE AICPA ALSO FOUND THAT ACCIDENTS OR NON-ROUTINE EVENTS TRIGGERED THE HIGHEST INCIDENCE OF DISCOVERY. IN FACT,

THE PROPORTION OF ACCIDENTAL/NON-ROUTINE DISCOVERIES IN THE INSURANCE CASES WAS CLOSE TO HALF, AS WAS THE CASE WITH THE PCIE STUDY.

THE DETAILS OF THE AMERICAN BAR ASSOCIATION (ABA) REPORT WILL, OF COURSE, BE DISCUSSED BY THEIR WITNESS TODAY. ALTHOUGH THE METHODOLOGY AND RESPONDENT POPULATION WAS VERY DIFFERENT FROM EITHER OUR PCIE SURVEY OR THE AICPA STUDY, IT IS INTERESTING TO NOTE A COUPLE OF GENERAL POINTS.

- WHILE ACKNOWLEDGING THAT RELIABLE STATISTICS DO NOT EXIST ON THE INCIDENCE OF AND LOSSES FROM COMPUTER CRIME, THE ABA REPORT DOES ASSERT THAT COMPUTER CRIME IS SIGNIFICANT AND GROWING.

- SECONDLY, THE ABA STUDY UNDERSCORES THE POINT THAT THE PCIE TASK FORCE MADE THAT AWARENESS, PARTICULARLY BY TOP MANAGEMENT, IS NOT AS HIGH AS IT SHOULD BE AND THAT LAW ENFORCEMENT PERSONNEL NEED MORE EXPERTISE TO INVESTIGATE AND PROSECUTE COMPUTER CRIME.

RECOMMENDATIONS OF THE PCIE STUDY

ALTHOUGH WE DID NOT CONSIDER OUR RESEARCH COMPLETE, WE DID MAKE SEVERAL RECOMMENDATIONS TO THE PCIE TO ADDRESS AREAS OF

IMMEDIATE CONCERN TO THE IG COMMUNITY. FIRST, BECAUSE THE RESPONDENTS, WHO WERE PRIMARILY INVESTIGATORS, APPARENTLY WERE UNFAMILIAR WITH THE STATE OF CONTROLS OR VULNERABILITIES IN THE VICTIMIZED SYSTEMS, WE RECOMMENDED INCREASED TRAINING AND AWARENESS. SECOND, BECAUSE SO MANY CASES WERE FOUND BY ACCIDENT, WE RECOMMENDED INCREASED SCRUTINY OF INTERNAL CONTROLS IN AUTOMATED SYSTEMS. WE TIED THIS TO THE REQUIREMENTS FOR VULNERABILITY ASSESSMENT AND INTERNAL CONTROL REVIEWS OF OMB CIRCULAR A-123, AND THE RISK ANALYSES REQUIREMENTS OF TRANSMITTAL LETTER NO. 1 TO OMB CIRCULAR A-71, WHICH IS NOW UNDER REVISION BY THE OFFICE OF MANAGEMENT AND BUDGET.

IN RESPONSE TO OUR RECOMMENDATIONS AND AS A RESULT OF INITIATIVES WHICH WERE ALREADY UNDERWAY, THE PCIE IS ADDRESSING THE TRAINING AND AWARENESS AND INTERNAL CONTROL CONCERNS IN SEVERAL WAYS:

- THE PCIE COMPUTER AUDIT COUNCIL, HEADED BY JUNE BROWN, THE NASA-IG, IS CHARGED WITH DEVELOPING CURRICULA FOR COMPUTER TRAINING OF BOTH AUDITORS AND INVESTIGATORS. IN ADDITION TO TRAINING THEM ON THE USE OF THE NEW GRID PORTABLE COMPUTER SYSTEM, THE COUNCIL HAS IDENTIFIED DIFFERENT TRAINING LEVEL NEEDS AND THE APPROPRIATE CURRICULA AVAILABLE TO MEET THESE NEEDS, WHETHER AT THE BASIC AWARENESS LEVEL (SUCH AS THAT NEEDED BY MOST

INVESTIGATORS) OR AT THE TECHNICAL EXPERT LEVEL. CERTAINLY IN MY OFFICE'S AUDITOR AND INVESTIGATOR TRAINING CLASSES, WE HAVE EXPANDED THE SECTIONS ON COMPUTER-RELATED FRAUD AND ABUSE AND ON THE IDENTIFICATION AND EVALUATION OF INTERNAL CONTROLS IN COMPUTER-BASED SYSTEMS.

- IN JUNE I CO-HOSTED WITH RICHARD H. SHRIVER, FORMER TREASURY ASSISTANT SECRETARY FOR ELECTRONIC SYSTEMS AND INFORMATION TECHNOLOGY, A ONE-DAY CONFERENCE ON COMPUTER SECURITY FOR INSPECTORS GENERAL AND ASSISTANT SECRETARIES FOR MANAGEMENT/ADMINISTRATION. WHILE THE TOPICS DISCUSSED RANGED FROM CURRENT MANAGEMENT AND IG INITIATIVES TO PRIVATE SECTOR TECHNIQUES AVAILABLE TO ADDRESS COMPUTER AND COMMUNICATIONS SECURITY PROBLEMS, ONE OF THE RECURRENT THEMES WAS HOW WE COULD WORK TOGETHER TO ADDRESS THESE PROBLEMS. THE INTERACTION AND CONCERN GENERATED IN THIS SESSION WAS PROBABLY MORE VALUABLE THAN THE TECHNICAL INFORMATION DISSEMINATED.

THE PCIE COMPUTER SECURITY PROJECT IS NOW IN THE MIDST OF SEVERAL IMPORTANT FOLLOWUP OR SPIN-OFF INITIATIVES, SINCE THE PCIE REPORT OF A YEAR AGO:

o PERPETRATOR INTERVIEWS - WE ARE CURRENTLY IN THE PROCESS OF INTERVIEWING THE COMPUTER-RELATED FRAUD PERPETRATORS WE FOUND IN OUR STUDY. WHILE IT IS STILL TOO EARLY TO DRAW ANY CONCLUSIONS, WE ARE FINDING THAT THESE INTERVIEWS CAN BE VERY REVEALING ABOU THE GENERAL VULNERABILITY OF OUR SYSTEMS IN ENVIRONMENTS WHERE SECURITY CONTROLS ARE INEFFECTIVE OR NONEXISTENT AND MANAGEMENT LACKS THE KNOWLEDGE, DESIRE OR TIME TO KNOW THAT IS HAPPENING AT THE WORKING LEVEL. A FEW PRELIMINARY CONCERNS (AND I STRESS THE WORD "PRELIMINARY") THAT HAVE EMERGED SHOULD BE OF INTEREST TO YOU:

--THE MAJORITY OF PERPETRATORS INTERVIEWED TO DATE PERCEIVE WEAK SUPERVISION OR LACK OF TECHNICAL SYSTEMS KNOWLEDGE OF THEIR SUPERVISORS AS VULNERABILITIES THEY WERE ABLE TO EXPLOIT.

--MOST OF THE PERPETRATORS INTERVIEWED THUS FAR HAD GOOD PERFORMANCE EVALUATIONS. INDEED, A FEW HAD RECEIVED AWARDS. THIS PRELIMINARY FINDING APPEARS TO COUNTER THE NOTION THAT ONLY POOR PERFORMERS ARE SUSPECT.

--A CERTAIN PROPORTION OF THE PERPETRATORS HAD PRIOR CRIMINAL RECORDS. WHILE IT IS TOO EARLY IN THESE INTERVIEWS TO BE MORE SPECIFIC OR ANALYZE THIS PRELIMINARY INDICATION, THIS DOES ALERT US TO THE POTENTIAL NEED TO REEVALUATE OUR PERSONNEL SECURITY PRACTICES AND PERHAPS INSTITUTE TIGHTER CLEARANCE PROCEDURES, AS YOUR SUBCOMMITTEE REPORT RECOMMENDED.

o EDP SYSTEMS REVIEW AND SECURITY ANALYSIS - THE PURPOSE OF THIS PROJECT IS TO INCREASE THE EFFECTIVE AUDIT REVIEW OF AUTOMATED INFORMATION SYSTEMS UNDER DEVELOPMENT TO INSURE THAT NEW SYSTEMS ARE INSTALLED WITH ADEQUATE INTERNAL CONTROLS, SECURITY FEATURES, AND AUDIT TRAILS. THE PROJECT WORK GROUP HAS DEVELOPED A RESPONSIBILITY MATRIX LISTING THE ROLES AND RESPONSIBILITIES OF KEY PLAYERS (INCLUDING AUDITORS) AND DOCUMENTATION NECESSARY THROUGHOUT A SYSTEMS LIFE CYCLE. THE RESPONSIBILITY MATRIX AND DOCUMENTATION GUIDE HAVE BEEN REVIEWED BY THE VAST MAJORITY OF INSPECTORS GENERAL AND SENIOR DATA PROCESSING MANAGERS IN THE MAJOR AGENCIES. COMMENTS HAVE BEEN QUITE FAVORABLE, INDICATING THAT THESE PRODUCTS WILL BE USEFUL TO BOTH THE IG AUDIT COMMUNITY AND MANAGEMENT IN THE PLANNING, DEVELOPMENT, AND INSTALLATION OF NEW AUTOMATED INFORMATION SYSTEMS OR MAJOR MODIFICATIONS TO EXISTING SYSTEMS. BUILDING ON THIS WORK AND ADDITIONAL

REVIEWS OF PRIVATE SECTOR APPROACHES. WE WILL DEVELOP A GENERALIZED AUDIT GUIDE, OUTLINING AN APPROACH TO REVIEWING SYSTEMS UNDER DEVELOPMENT AND ENUMERATING KEY AREAS OF AUDIT CONCERN.

- ELECTRONIC MEDIA BILLING - THIS PROJECT IS REVIEWING THE PROCESS OF ELECTRONIC TRANSMISSION OF HEALTH PROVIDER CLAIMS TO GOVERNMENT HEALTH CARE FINANCING PROGRAMS (I.E., MEDICARE, MEDICAID AND CHAMPUS). THIS REVIEW, WHICH WILL ISSUE A FINAL REPORT IN THE NEAR FUTURE, FOUND THAT ALTHOUGH FORMAL COST-BENEFIT ANALYSIS HAD NOT BEEN DONE, ELECTRONIC MEDIA BILLING APPEARED TO BE A MORE EFFICIENT PROCESS THAN MANUAL BILLING. HOWEVER, THE REVIEW ALSO FOUND THAT THE PROCESS CONTAINS SEVERAL VULNERABILITIES (SUCH AS A WEAK CERTIFICATION PROCESS) AND NEEDS GREATER STANDARDIZATION OF FUNCTIONS AND CONTROLS.

IN ADDITION TO THESE ACTIVITIES, FUTURE TASKS OF THE PCIE COMPUTER SECURITY PROJECT INCLUDE ANALYSIS OF THE FEASIBILITY OF MAINTAINING AN ONGOING DATA BASE OF COMPUTER-RELATED FRAUD AND ABUSE CASES AND AN ASSESSMENT OF THE CURRENT STATE OF SECURITY IN VICTIMIZED SYSTEMS IDENTIFIED IN OUR SURVEY.

MR. CHAIRMAN, I THANK YOU FOR THE OPPORTUNITY TO OUTLINE OUR ACTIVITIES AND DEVELOPMENTS TO DATE. THIS CONCLUDES MY PREPARED STATEMENT. I AM AVAILABLE TO ANSWER ANY QUESTIONS YOU MAY HAVE.

COMPARISONS OF COMPUTER CRIME STUDIES

PERPETRATORS

	PCIE		AICPA		ABA
	FRAUD	ABUSE	BKG	INS	
USER	62 %	30 %	82 %	88 %	38 %
DPER	30	59	14	3	82
OTHER	8	11	4	9	11

(MULTIPLE ANSWERS ALLOWED)

SOURCES: PCIE - INSPECTOR GENERAL, U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, "COMPUTER-RELATED FRAUD AND ABUSE IN GOVERNMENT AGENCIES," JUNE 1983.

AICPA - EDP FRAUD REVIEW TASK FORCE, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, "REPORT ON THE STUDY OF EDP-RELATED FRAUD IN THE BANKING AND INSURANCE INDUSTRIES," 1984.

ABA - TASK FORCE ON COMPUTER CRIME, SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION, JUNE 1984.

COMPARISONS OF COMPUTER CRIME STUDIES

LOSSES

	PCIE	AICPA		
	(FRAUD)	BKG	INS	ABA
NONE - $100,000	93 %	86 %	79 %	65 %
OVER $100,000	7	14	21	7

COMPARISONS OF COMPUTER CRIME STUDIES

DETECTION

WHO DETECTED?

	PCIE		AICPA	
	FRAUD	ABUSE	BKG	INS
OPERATING STAFF	55 %	68 %	51 %	68 %
OVERSIGHT STAFF	28	20	29	15
OTHERS	17	12	21	18

COMPARISONS OF COMPUTER CRIME STUDIES

DETECTION

HOW DETECTED?

	PCIE		AICPA	
	FRAUD	ABUSE	BKG	INS
ACCIDENT/NONROUTINE EVENT	49 %	51 %	31 %	47 %
CONTROLS	25	24	14	29
AUDIT	26	25	20	12
CUSTOMER	--	--	28	12
UNIDENTIFIED	0	0	7	0

Mr. GLICKMAN. The next witness is Mr. Robert Campbell, president of Advanced Information Management, Inc.

Mr. Campbell—you are Mr. Campbell—right? A pleasure to have you here, and why don't you go ahead and begin, and, as I said, if you want to summarize your statement, I don't know how long it is, but you feel free to do so, so we'll have time to ask you and our final witness plenty of questions.

STATEMENT OF ROBERT P. CAMPBELL, PRESIDENT, ADVANCED INFORMATION MANAGEMENT, INC., WOODBRIDGE, VA, ACCOMPANIED BY BRUCE E. SPIRO, CHIEF, ADP SYSTEM MANAGEMENT, DEFENSE COMMUNICATIONS AGENCY

Mr. ROBERT CAMPBELL. Thank you, Mr. Chairman.

I will summarize. I would request that my full statement be entered into the record.

I'm accompanied today by Mr. Bruce Spiro of the Defense Communications Agency, who is also president of the Data Processing Management Association Education Foundation and chaired the DPMA committee that developed its code of ethics and standards of conduct, which we will be discussing later on.

I would like to express my personal admiration to the committee for continuing its work. I believe this is a subject that we've just only begun to address, and I support your report and your recommendations and hope that you continue to press on on the subject.

I've approximately 20 years of experience in the Federal Government environment and another 6 years of experience in the commercial environment, involving some of the most sensitive and critical systems in both sectors. I'd like to try to convey some of that perspective here this afternoon.

I believe the first point that comes to my mind is that regarding the threat. I believe there is a tendency to misunderstand or misjudge the level of the threat. I believe that our image of the threat—the long-term threat may not be accurate.

Threat is not static; the level of threat has and will continue to be difficult to define. I believe that we have to go after it with more intensity in order to be able to stay on top of the situation.

We're walking a very fine line between the threat and our ability to defend against the threat. The danger in this, I believe, lies in our inability to sense in real time or in enough time to respond accurately changes in the nature of the threat.

I believe our policies in this area are inconsistent in that, at the Federal level, we require the agencies and departments to have a formal risk analysis program, but yet at the national strategic level we are not maintaining the same formal level of sensitivity.

I previously suggested that there be a blue ribbon commission to assess the strategic national vulnerability caused by our increasing dependence upon untrustworthy computer systems.

I believe that we are inclined to ignore the indicators of problems, the postulated threats that should be tipping us off to take some more decisive action.

I believe a commission chartered to look into these vulnerabilities, to identify the issues and develop strategic alternatives—we

need a strategy to focus ourselves in the long term. I believe this is an absolute necessity.

This is nowhere more acutely manifested than in the area of computers versus communications. This is an area where we still have not girded our national policies to focus uniformly upon the problem and put forth a strong resolve.

The difference between communications and computers is going to be moot. The differences are going to be immaterial to the long-term solution of the—the problem.

Another area that I would like to address, having looked at both sides of the picture, is that concerning lack of economic viability in computer security. The most frequent comment that I receive back in regards to security is that it does not make economic sense.

My respected colleague, Willis Ware, was party to a study that was published in 1969—15 years ago—which documented the vulnerabilities in the Federal Government. In the intervening 15 years, the collective economic and political influence of the Department of Defense, the intelligence agencies and the Federal Government, have been inadequate to buy this trustworthy technology.

I think this is a question that we have to look into to determine whether that 15 years was justified and whether it's going to take another 15 years to satisfy these requirements.

As a result, our Defense needs have had to be satisfied primarily through the use of off-the-shelf and untrustworthy type of technology.

There's a revolution taking place in the private sector regarding the use and application of computer systems. What were once internal administrative systems are now being used commercially as profit centers to deliver the information utility, to provide services, valuable assistance, for profit, to users outside of the immediate organization.

What this tells me, or what we're seeing, is that systems that once could be physically and environmentally sheltered are now moving outside of that shelter and are becoming more dependent upon the logical rather than the physical controls.

We do not see the logical controls as adequate to the needs at hand.

We were approached by a large manufacturing organization on behalf of their management who were about to field a new system that would take the human element out of the order-entry process.

In this scenario, the prospective client would previously call an order-entry clerk and inquire as to the availability of—of goods, materials, how long it would take to manufacture them, and the status of an order.

The management of that organization required that before that system could be put into operation, that the proponents of the system satisfy management that people coming in from the outside of the organization could not, one, access sensitivity organization information; or, two, could not access the information of competitor organizations who were also ordering from that corporation.

What we are clearly seeing is a statement of capabilities arising out of the commercial sector which is largely mirroring those put forth by Dr. Ware some 15 years ago.

We repeatedly hear about economic viability. The direction of computer security has been almost totally established in terms of economic viability, and until it is viewed as something that will sell, the vendors will not provide the stimulus to the marketplace.

Now these are the contentions of the vendors and the practitioners, who, in my opinion, are not the riskers. The real riskers are the citizens, the functional users of the systems, and our national institutions. They lack the voice or representation to move the problem.

I recommended in my testimony the foundation of a computer communications security research organization that would be able to set aside vested interest, short-term profit motivation, economic viability, and focus upon the public good and its long-term needs.

I believe that Congress is the only organization that can act in the public interest to cut through the heart of the problem and create the environment that can make these things happen.

In the area of ethics and professionalism, I have been serving for the last almost 2 years as president of the Institute for Certification of Computer Professionals, which is an organization that was chartered in 1973 by eight major data processing societies to act on behalf of the profession to test and certify knowledge of computer professionals.

As part of this certification process, we require that all certificants subscribe to the ICCP code of ethics, code of conduct, and good practice.

In the 20 years of the data processing profession, it has not, except under—except under one circumstance, been able to police itself and withdraw the rights of a member due to a violation of the code of ethics. I'm proud and pleased to say that the ICCP is the organization that has done that.

In a very lengthy and time-consuming process fraught with potential liabilities for the board, the members of ICCP and its managing body, we succeeded in withdrawing the certification of an individual who had violated our code of ethics.

We believe that voluntary certification and adherence to a code of ethics is a powerful mechanism to guide us in this period of technological shortcoming, systemic vulnerabilities, and high public dependence.

We are now and will be for a long time extraordinarily beholden to the good auspices of a large number of people who occupy positions of exceptional privilege and high trust in the application, operation, and use of these computer systems. Security clearances and background investigations are not enough. A high state of ethical conduct is imperative.

I feel the industry and profession have failed to deal effectively with the vitalness of ethics in the evolution of the technology. We failed to develop the essential ethical base amongst our purveyors and practitioners prior to moving the technology into the public domain, and I believe that's why we're seeing the incidence of abuse that we are.

With this, I think we have violated an implicit faith that has been placed in us by allowing unsecure systems to develop. We're dealing with a national attitude that we have helped to create, a situational ethic with—which ought not to be tolerated.

The recent penetration of a large credit database, I think, illustrates this. The penetration itself was not a difficult technical challenge. The response of the credit bureau was to state that no harm had been done since their system had been designed to allow outsiders only to read and not to change records.

I find this situation intolerable but a reflection of a situational ethic which we have fostered by our failure to act responsibly in this area.

Despite what the technocrats say, there are serious deficiencies in the technology and its application.

Most large corporations, since the technology is inadequate and they are unable themselves to overcome the deficiencies, must operate as best they can, and I think this is a type of ethical compromise which has become routine and nationally condoned by inaction.

We have created the ethical compromise and are allowing it to perpetuate under the guise of lack of need, lack of economic viability, lack of evidence of threat, and other similar logical illusions.

Your committee accurately identified this area as one of the most complex that we have had to face. I agree with this. I believe that we are still dealing largely with symptoms and obvious effects rather than root causes.

The problem itself is cyclical in nature. In the period of time that I've been involved, I've watched the problem come to the fore every 4 or 5 years and then recede.

I think it's imperative at this point that the problem continue to be given the type of visibility that will lead to its solution.

Mr. Chairman, thank you.

Mr. GLICKMAN. Thank you.

You talked about the certificates for computer professionals. Does anybody in industry use those certificates in their hiring?

Mr. ROBERT CAMPBELL. Certification has not caught on within industry. We occasionally will see in job ads requests for individuals who hold the certification. Sometimes we will see a certificate in data processing or a master's degree equated, but the certification itself, as a valuable credential, has not yet gained acceptance within the industry.

Mr. GLICKMAN. OK. Let me ask you this question. You've—have you been here the entire day and listened to the other witnesses?

Mr. ROBERT CAMPBELL. Yes, I have.

Mr. GLICKMAN. From your experience in the private sector, would you agree with OMB's overall—I categorize them as "rosy assessment" of computer security in the Government?

Mr. ROBERT CAMPBELL. No, Mr. Chairman, I cannot subscribe to any rosy assessment of computer security in the Government. I believe that in many ways the Government is lagging the private sector in its efforts to deal with computer security.

I don't know really why this is so. I believe it has its roots in our previous attention to the protection of classified systems. I believe it also has its roots in the inability to adequately sense the sensitivity or criticality of systems that are not classified.

I feel we have a great deal of work to do in this area yet before we are attuned to the level of sensitivity and criticality of these systems.

If we have not yet an adequate inventory of our resources, if we don't know what they're doing that's sensitive and critical, then there's no way we can mount an effective campaign to protect them.

Another aspect of the—of the problem—and it's reflected in the difference between the private sector and the Federal Government—has been the past inclination of the government to focus upon motivation. The security clearance process, the background investigation, has given us a feeling of comfort that once a person has become vetted, they then are trusthworthy and privileged to the system.

In the private sector, this process does not take place. Consequently, the emphasis has shifted from motivation to opportunity, and we see a great deal more effort being put into reduction and elimination of the opportunity rather than an attempt to predict an individual with motives.

Mr. GLICKMAN. A final question. You talked a little bit about a foundation in your statement. Who would participate in this foundation, and would it be research-oriented?

Mr. ROBERT CAMPBELL. Its focus would be to create a research or needs agenda. I believe the participants would probably come heavily from the private sector but also be represented from the Federal Government sector.

My experience in participating in many, many workshops with many different functional groups and associations has been that we're all basically asking for the same thing, but there is no one that can take that and overlay it into a statement of capabilities and requirements and then further take it into a research and development agenda that we can work with.

Similarly, once the technology has been created, I think we're lacking that foundation to promote its application.

The data incryption standard promulgated in 1977 is an—is an excellent example. It is the technology to take care of the problem of protecting sensitive information in transit. However, its application effectively is still not with us.

I believe that a research foundation would have the capability of bringing all these parties together, allowing them to express their interest, and convey them to the people that can address them.

There is no advocacy group in the private sector, and this, I think, is a serious problem.

Mr. GLICKMAN. Mr. Campbell, we thank you very much for your testimony today.

[The prepared statement of Mr. Campbell follows:]

TESTIMONY OF

ROBERT P. CAMPBELL, CDP

PRESIDENT,
ADVANCED INFORMATION MANAGEMENT, INC.

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

September 24, 1984

I. INTRODUCTION

My name is Robert P. Campbell. I appreciate the opportunity to appear before this Subcommittee to discuss the subjects of computer and communications security and privacy. My purpose is to share with you my views on the nature and magnitude of the threat to computer security and privacy; the need for a computer and communications security research foundation to help focus national thinking about the problem; and to discuss my involvement in developing a program for certifying computer professionals and the ethics related aspects of that program.

I would like to express my personal admiration for this subcommittee's continuing efforts in this vital area. The problem desperately needs national attention and right now. This subcommittee is the main hope that we have for this attention. I note that on the occasion of the passage by the House of Representatives of H.R. 5616 on July 24, 1984, you, Mr. Chairman, were one of the few speakers to acknowledge the need for additional action. I strongly support the Subcommittee's report and recommendations.

I am President of Advanced Information Management, Incorporated, a small business which I founded just over five years ago. We consult exclusively in the area of computer and telecommunications security, privacy and disaster recovery planning. Our client base is comprised of three of the top ten banks in the United States, and top ten firms in financial services, credit card, mutual fund, stock brokerage, oil, insurance, and manufacturing industry groups, as well as one of the major stock exchanges. We have also done considerable work for leading Federal government departments and agencies.

Prior to founding my company, I served twenty years with the United States Army in a variety of intelligence and data processing assignments. While on the Department of Army staff, I was the developer and program manager for the Army's Automation Security Program as well as the

architect and principal author of Army Regulation 380-380, Automated Systems Security, the first and most comprehensive such policy document promulgated by any department of the United States government.

This unique combination of experience has given me twenty-six years of involvement with some of the most sensitive and critical systems in both the Federal government and private sector.

II. NATURE AND MAGNITUDE OF THE THREAT

I am concerned that the public and thus our national image of the computer security threat is of fun-loving school children innocently and without malice accessing our sensitive systems. We should make no mistake that our sensitive systems, government and private, are and will be increasingly under attack. They are the target of determined and skilled adversaries, both foreign and domestic, because of the great potential for gain or benefit. Unfortunately, this same attractiveness will also appeal to increasing numbers of trusted system users and operators as the value of the systems and opportunities to exploit them increase.

Threat is an extremely difficult subject with which to deal. As a former intelligence officer, I am accustomed to dealing with intelligence indicators and postulated threats as they relate to national security. A postulated threat is one which appears quite feasible but which has yet to surface or be detected. An indicator is an identified event which might reveal the existence of a threat.

A threat is represented by any individual or group motivated to take advantage of our systems for their gain and conversely, our loss. Because motivation is hard to predict where the potential for loss is great, motivation must be either assumed or the threat closely monitored for occurance. The other side of this equation is opportunity. Where the opportunity presents itself, due to a concentration of valuable resources, a lack of security controls or both, we would be naive not to expect someone to seek advantage.

From this perspective, I see the course we are taking in computer security to be fraught with danger. Our nation is walking a fine line in balancing the threat, foreign and domestic, with our response to the threat. We are engaging in a point-counterpoint relationship with the threat which requires a very delicate equilibrium. The fallacy of this approach is that we lack the mechanisms to anticipate or sense a shift in this balance or to detect the indications of an increase in the level of the threat. In fact, the current mind set of our leadership favors ignoring these indicators and postulated threats until the hard evidence becomes incontrovertible and undeniable. We seem to be seeking excuses not to act. This lack of commitment leaves us in a highly vulnerable strategic national position.

III. OUR CONFUSED NATIONAL POLICIES

We are inconsistent in our behavior. For example, our highest national policies in the area of computer security require Federal agencies to implement a formal, ongoing risk analysis program for their sensitive and critical systems. However, we have failed to do the same at a national strategic level on behalf of the government, its private institutions and its citizens I believe this is a shortcoming which must be corrected.

Our policies lack credibility because they are unfunded, impractical and unenforceable. Security policy requires risk analysis but provides no meaningful guidelines on how to perform risk analysis. Millions of dollars have been squandered by government agencies thrashing in reaction to this policy. The same can be said for the policies regarding contingency planning and audit of computer systems. Common problems require common solutions derived from strong central leadership.

IV. A BLUE RIBBON COMMISSION

Other than for national security information, our policies and guidelines regarding protection of other types of sensitive unclassified information and systems are disjointed and ineffective. Stronger, more

cohesive policies here would energize a large segment of the Federal establishment, presently inert, to get behind government R&D efforts and define their needs. Your recommendation of a classification or categorization schema for non-defense information is an important step in this area.

Four years ago, I publicly called for a Blue Ribbon commission to assess our strategic national vulnerability caused by overwhelming dependence upon untrustworthy computer systems. That need is no less today. It is perhaps greater, because despite the revelations of computer vulnerabilities, abuses and subsequent investigations, we still have not developed the national resolve and direction to deal effectively with the problem. We are ignoring the indicators, the postulated threats which should be sufficient cause for us to act. This national commission is an important first step and therefore I strongly support the recommendation you have made in this area. This Commission, chartered to assess our vulnerabilities, identify issues and develop strategic alternatives, is an absolute necessity in my view, in order to firm our national resolve. The void in national commitment, direction and leadership is extremely serious. Nowhere is it more critical than in the vestiges of the computers versus communications controversy and the political battlelines that have been drawn. The positions of both Presidential Directive 24 and OMB Circular A-71, Transmittal Memo Nr. 1 epitomize this. The confrontation is now moot and overtaken by events; the technology has blurred the differences; the logical environment makes proponency transparent. These differences must be put aside in favor of an effective unified national policy. We are already years past the point where this policy should have been effected. Lesser solution will have us meeting again in a few years to further lament the lack of leadership and direction.

V. SECURITY IS NOT YET ECONOMICALLY VIABLE

My respected colleague, Willis Ware of Rand Corporation, who spoke to you last year, was party to a study of computer system vulnerabilities

conducted on behalf of the Defense Science Board in the late 1960's. This classic work detailed system vulnerabilities and set the stage for Defense policies and programs for the next decade and a half. This document is as current today as it was in 1969. It clearly set the challenge be met in developing trustworthy and secure technology. However, despite this early recognition of need, in the intervening fifteen years, the collective economic and political clout of the Department of Defense, Intelligence Community and Federal government have been inadequate to buy this trustworthy technology. We should take little consolation in the fact that our highly classified computer systems were spared public embarrassment during the "hacking" onslaught last year. Their security has been achieved by a national policy of isolation and segregation which only leads to serious operational sacrifices and will eventually limit our strategic national defense capability.

The computer industry has long felt that these requirements were unique to Defense and the resource investment to meet these needs was not justified. Clearly and simply, it was an economic decision which has resulted in the government having to use off-the-shelf equipment with whatever security attributes the industry provided. As we have seen, the technology has not provided the type of trustworthy systems necessary to allow us to change our isolation policy. Industry has failed to respond to these needs primarily because they were perceived to be Defense unique and not economically viable. However, I am hard pressed to fault the computer industry because the economic investment to provide this technology is beyond the perceived risk threshold of any single vendor and perhaps even the industry, without clearer definition of need or more extensive research and development, especially by the government.

VI. SECURITY IS IN THE PUBLIC INTERESTS.

However, what is currently happening in the private sector is proving the premise of Defense uniqueness to be inaccurate. The spread of the technology over the past five years in the private sector has been dramatic. Systems which a decade ago were supporting administrative needs have matured and been dramatically integrated into essential business

operations. The rapid evolution of both computer and communications technology has now removed the physical restraints from these systems, to the extent that these same internal support systems and mechanisms are now being used to convey information and services to external clients and customers. These systems, which originally could be afforded physical and environmental protections so as to guard against intrusion by outsiders, are now being used to deliver goods and services to end users at curbside or in their homes. The ability to clearly separate "insiders" and "outsiders" physically has given away to the need to separate them logically within the system. These systems are currently not equal to this task and will not be for a considerable period of time. These needs virtually mirror those established by the Defense community ten years ago.

VII. PUBLIC INTERESTS VS. ECONOMIC VIABILITY

The direction of computer security has been set almost exclusively in terms of economic viability. We hear repeatedly that security has not and will not sell. Vendors continue to insist that there is not yet a demand for security in the marketplace. These are the contentions of the vendors and data processors, who are not the riskers. The real riskers are the citizens and our national institutions. They, however, lack the voice or representation to move the problem. When the cost/benefit analyses are done, who will represent the people? Who is looking out for our public interests? I have no great comfort that these interests are being served.

VIII. A COMPUTER/COMMUNICATIONS SECURITY FOUNDATION

I believe then that a large measure of the solution lies with a group that can set aside vested interests, the short-term profit motivation, economic viability and focus upon the public good and its long-term needs. I believe that Congress is the only body that can act in the public interest to cut through to the heart of the problem and create

favorable environment which can make things happen. One of the mechanisms for this is, in my opinion, a congressionally-chartered, non-profit computer/communications security research foundation or similar mechanism.

The notion of the Foundation was originated about five years ago by myself and a group of colleagues. After participating in numerous security workshops sponsored by banking, insurance, privacy, government, professional, legal, audit and security groups, we noted that they were all saying the same thing but lacked the advocacy group to put it together. There was no mechanism to collect all of their needs into a requirements or research agenda or to move the technology into practical application. An excellent example of problems moving the technology to practical application is the Federal Data Encryption Standard (DES). While the technology of the DES has been available since 1977, the problems in its application still prohibit its widespread use. A broader base of validated requirements and support constituency would accelerate this process. A broadly based, validated research agenda is imperative if we are to be responsive to our national needs in this exploding technology.

IX. THE INSTITUTE FOR CERTIFICATION OF COMPUTER PROFESSIONALS

I have also been asked to testify on the ethics-related aspects of the certification programs of the Institute for Certification of Computer Professionals (ICCP). I am currently serving as President of ICCP, an elected position that caps eight years of direct professional commitment to certification. The ICCP is a not-for-profit umbrella organization established in 1973 by eight major data processing professional associations to test and certify knowledge of computing personnel in a coordinated, cooperative industry-wide effort.

The Institute currently offers two major certification programs:

> Certificate in Data Processing (CDP) for business-oriented data processing personnel at the management and supervisory levels.

Certificate in Computer Programming (CCP) for senior level computer programming personnel in the business, scientific and systems programming areas of specialization.

Since the first CDP examination was given in 1962 under the auspices of the Data Processing Management Association, more than 24,000 successfully achieved a Certificate in Data Processing. A record 4,237 candidates sat for the May 1984 CDP exam which was given in 165 sites in the United States, Canada and 17 countries in Europe, Africa, Asia and Latin America. More than 2,000 professionals currently hold the CCP.

These professional certification programs were intended to be the data processing profession's equivalent to the CPA in the accounting profession.

All certificants must subscribe to the ICCP Code of Ethics, Conduct and Good Practice. A number of professional societies have codes of ethics; most lack enforcement mechanisms. However, the codes of both the ICCP and one of its constituent societies, the Data Processing Management Association (DPMA) do have enforcement procedures. Copies of both codes are provided as attachments to this document. Enforcement is a very difficult process. However, I am pleased and proud to say that the ICCP is the only organization in the profession to have taken action against a member for violation of its Code of Ethics.

In a very lengthy and involved process, the Institute completed proceedings in 1981 leading to the withdrawal from an individual of its Certificate in Data Processing. Spearheaded by Dr. Coleman Furr, President of Coleman College and Head of our CDP Certification Council, it was a difficult and time consuming process fraught with potential liabilities for the Institute, its Officers and Board, despite the fact that the individual had been tried and convicted of a criminal act involving specialized knowledge of the technology and its application.

In this case identifying the specific provision of the ethical code that was violated was relatively easy. It was very difficult citing the

specific code of conduct and good practices that had been violated, primarily because they lacked proper depth and definition. Enforcement of a Code of Ethics is an area requiring an exceptionally well defined standard of practice and expected behavior, which can be applied much like the rules of evidence and elements of proof in a court of law. The Institute has had a validated requirement to define its codes of good practice into a useful enforcement vehicle for the profession for a number of years but has lacked the resource base to do so.

Right now, the Institute's base of economic support comes primarily from the individual seeking certification and, to a limited extent, from the professional societies. We are also seeing slowly increasing support from companies employing computer professionals. However, the individual is bearing the load in the development of this certification program on behalf of the profession and industry. This is not right. I am sorry to say that we have had virtually no direct support from the computer industry, the purveyors of the technology. Our effort to have the credentials recognized by the Federal civil service were previously rejected but we are trying again to draw government support. I have taken action to establish a separate non-profit Foundation for the Institute so as to establish favorable tax status and thus facilitate corporate contributions in an effort to overcome this deficiency and allow us to pursue our programs to their fullest extent. Our application for this status is currently pending.

X. THE ROLE OF PROFESSIONAL ETHICS

We believe voluntary certification and adherence to a code of ethics to be powerful mechanisms to guide us during this period of technological shortcomings, systemic vulnerabilities and high public dependence . We are now and will be for a long time extraordinarily beholden to the good auspices of a large number of people who occupy positions of exceptional privilege and high trust in the application, operation and use of these computer systems. Security clearances and background investigations are not enough. A high state of ethical conduct is imperative if individuals are to turn away from the great temptations which will be presented as

systems become more valuable and critical to our every day life. Until such time as the technology of security and control evolves to the point where these extraordinary "opportunities" no longer exist, we must have this exceptional trustworthiness in people to make up for the lack of such in the systems.

The industry and profession have failed to deal effectively with the vitalness of ethics in the evolution of the technology, failing to develop an essential ethical base amongst its purveyors and practitioners. The technology has now moved into the public domain in the form of personal or home computing without this essential ethical base migrating with it. It is not surprising that we are now seeing dramatic abuses of the technology. What are the ethical issues behind these attitudes and those that allow the implementation of sensitive systems without adequate system security and control? There is danger in the attitudes that are allowing these vulnerable systems to exist. Much of the rationalization of the youthful hacker is based upon the notion that if it was that important, society and its institutions would not let it happen. I believe that our national leadership has violated an implicit faith that society has placed in us by allowing these unsecure systems to develop. We are dealing with a serious national attitude which we have helped to create, a situational ethic which ought not to be tolerated.

Recent revelation of penetration of a large credit data base typifies this situation. Outsiders were able to gain access to sensitive credit information on individual citizens. It was not a difficult technological challenge. The response of the credit bureau was that no harm had been done since their system had been designed to allow outsiders only to read and not change records. As a private citizen, I find this situation intolerable, the reflection of a situational ethic which we have fostered by our failure to act responsibly. However, as a security person, I am hard pressed to completely fault the credit bureau. It is performing a valuable function for us as a society, it has applied the technology to its fullest extent and has acted with great sensitivity to the laws of the U.S. In fact, I somewhat admire the cleverness with which this company and many others are trying to work around technological shortcomings.

Despite what the technocrats say, there are serious deficiencies in the technology and its application. Our technical inability to identify, separate and isolate users and data in common systems and networks underlies the problems in the credit bureau scenario. If they are to do business, they must do so within the bounds of the technology provided to them. Since the technology is inadequate, and they are unable themselves to overcome the deficiencies, they must operate as best they can. This type of ethical compromise has become routine and nationally condoned by our inaction. We, as an institution, have created the ethical compromise and are allowing it to perpetuate under the guise of lack of need, lack of economic viability, lack of evidence of threat and other similar logical illusions.

XI. WE ARE STILL DEALING WITH SYMPTOMS

You accurately identified this area as having an array of multifaceted issues of a complexity and multijurisdictional character, that are unlikely to be dealt with effectively by any single organization or committee. In addition, even after the visibility this problem has been given, I feel that we are still dealing largely with symptoms and obvious effects rather than root causes. We must redouble our efforts to seek the underlying causes and issues in order to gain solution.

Here again, we are at a critical point. I have observed over the years the cyclical nature with which the problems of computer and communications security are given visibility. Every 4-5 years there is official attention and media interest, then the level of interest quickly wanes, without adequate action being taken. I see this interest rapidly waning again. But for your committee, the problem and its symptoms would once again recede for a few more years. Management is often inclined to feel that, having exposed a problem, its resolution is a matter of natural course. Perhaps so, but in this case, we must tenaciously continue to delve into and understand this problem. The stakes are too high not to.

BIOGRAPHY

ROBERT P. CAMPBELL, CDP, is President of Advanced Information Management, Incorporated, a private international consulting firm specializing in computer and telecommunications security, privacy and contingency planning. During over twenty years of data processing, security and audit experience in both government and industry, he pioneered many innovative techniques for protecting automated systems and managing computer security risks. An experienced manager, his achievements range from the development of corporate-wide computer security programs, the development of detailed computer security and audit policy and procedural manuals, to devising technical security controls for complex computer networks. He has counseled senior management of numerous Fortune 500 companies on security, privacy and fraud issues.

As a recognized international authority in these areas, he has been widely referenced in such major news media as Time, U.S. News, Business Week, network television, most large daily newspapers and trade publications. He has lectured extensively and has participated in numerous international invitational forums on the subject, to include the distinguished Brookings Institution Computer Crime and Privacy National Issues Seminar, National Bureau of Standards' Invitational Workshop on Audit and Evaluation of Computer Security, the American Federation of Information Processing Societies (AFIPS) Invitational Workshop on Computers and Privacy, and the EDP Auditors Foundation's Workshop on Auditing Systems Software and Its Control Objectives Workshop. He was also Conference General Chairman for the major international Computer Crime Info - Computer Security and Fraud Control Conference held in Washington, D. C., in December, 1980. A frequent and widely published writer, his most recent works are a comprehensive "Guide to Automated Systems Security," a widely-acclaimed COMPUTER-WORLD feature "Locking Up The Mainframe," and contributed articles for Wiley's "Advances in Computer Security Management, Vol. II" and Auerbach's "Data Security Management" portfolio.

Professionally active, he has served on the Board of Directors and is currently President of the Institute for Certification of Computer Professionals (ICCP), the Program Committee of 1979 National Computer Conference, the AFIPS Committee on Right to Privacy, as a national director of the Association of Computer Programmers and Analysts and on the editorial advisory boards of the Computer Security Journal (U.S.), Computer Fraud and Security Bulletin (U.K.) and Corporate Crime and Security Bulletin (U.K.). In addition, he writes a monthly column on Computer Security for Government Computer News (U.S.). He holds a B.A. in Business Administration from St. Lawrence University and a M.B.A. with specialization in data processing from American University.

INSTITUTE FOR CERTIFICATION OF COMPUTER PROFESSIONALS

codes

of ethics, conduct and good practice for certified computer professionals

Institute for Certification of Computer Professionals
35 East Wacker Drive • Chicago, Illinois 60601

© copyright 1977,

Institute for Certification of Computer Professionals
35 East Wacker Drive
Chicago, Illinois 60601

Certified computer professionals are a select group of people who have qualified for and successfully completed an examination assessing their grasp of the knowledge considered by recognized experts as important to the area in which they are certified.

The ICCP has consistently, throughout its existence, recognized the need for a set of personal and professional standards to support and identify those individuals dedicated to the quest for knowledge and competence, to ethical behavior and social responsibility, and to the advancement of the computer profession. By choosing to seek certification, Certificate holders have demonstrated their concern for the continuing development of high standards of personal and professional conduct.

The following pages contain the Codes of Ethics, Conduct and Good Practice adopted by ICCP at its inception. These Codes are guidelines to which all Certificate holders subscribe and follow in the execution of their responsibilities.

ICCP also recognizes that violation of the Codes of Ethics, Conduct and Good Practice by any Certificate holder is an act contrary to the principles of the certification program and a breach of the requirements for certification. Therefore, the ICCP has reserved for and delegated to each Certification Council the right to revoke any Certificate issued under a Council's administration in the event that the Certificate holder violates the Codes of Ethics and/or Conduct or otherwise engages in conduct which is a discredit or disgrace to the computer profession. The revocation procedures approved by the Certification Councils are also included in this booklet.

The certification programs of ICCP represent a significant effort to promote high standards of excellence for members of the computer profession.

CODE OF ETHICS FOR CERTIFIED COMPUTER PROFESSIONALS

Certified computer professionals, consistent with their obligation to the public at large, should promote the understanding of data processing methods and procedures using every resource at their command.

Certified computer professionals have an obligation to their profession to uphold the high ideals and the level of personal knowledge certified by the Certificate held. They should also encourage the dissemination of knowledge pertaining to the development of the computer profession.

Certified computer professionals have an obligation to serve the interests of their employers and clients loyally, diligently, and honestly.

Certified computer professionals must not engage in any conduct or commit any act which is discreditable to the reputation or integrity of the computer profession.

Certified computer professionals must not imply that the Certificates which they hold are their sole claim to professional competence.

CODES OF CONDUCT AND GOOD PRACTICE FOR CERTIFIED COMPUTER PROFESSIONALS

The essential elements relating to conduct that identify a professional activity are:

A high standard of skill and knowledge.

A confidential relationship with people served.

Public reliance upon the standards of conduct and established practice.

The observance of an ethical code.

Therefore, these Codes have been formulated to strengthen the professional status of certified computer professionals.

1. Preamble

1.1: The basic issue, which may arise in connection with any ethical proceedings before a Certification Council, is whether a holder of a Certificate administered by that Council has acted in a manner which violates the Code of Ethics for certified computer professionals.

1.2: Therefore, the ICCP has elaborated the existing Code of Ethics by means of a Code of Conduct, which defines more specifically an individual's professional responsibility. This step was taken in recognition of questions and concerns as to what constitutes professional and ethical conduct in the computer profession.

1.3: The ICCP has reserved for and delegated to each Certification Council the right to revoke any Certificate which has been issued under its administration in the event that the recipient violates the Code of Ethics, as amplified by the Code of Conduct. The revocation proceedings are specified by rules governing the business of the Certification Council and provide for protection of the rights of any individual who may be subject to revocation of a Certificate held.

1.4: Insofar as violation of the Code of Conduct may be difficult to adjudicate, the ICCP has also promulgated a Code of Good Practice, the violation of which does not in itself constitute a reason to revoke a Certificate. However, any evidence concerning a serious and consistent breach of the Code of Good Practice may be considered as additional circumstantial evidence in any ethical proceedings before a Certification Council.

1.5: Whereas the Code of Conduct is of a fundamental nature, the Code of Good Practice is expected to be amended from time to time to accommodate changes in the social environment and to keep up with the development of the computer profession.

1.6: A Certification Council will not consider a complaint where the holder's conduct is already subject to legal proceedings. Any complaint will only be considered when the legal action is completed, or it is established that no legal proceedings will take place.

1.7: Recognizing that the language contained in all sections of either the Code of Conduct or the Code of Good Practice is subject to interpretations beyond those intended, the ICCP intends to confine all Codes to matters pertaining to personal actions of individual certified computer professionals in situations for which they can be held directly accountable without reasonable doubt.

2. Code of Conduct

2.1: Disclosure: Subject to the confidential relationships between oneself and one's employer or client, one is expected not to transmit information which one acquires during the practice of one's profession in any situation which may harm or seriously affect a third party.

2.2: Social Responsibility: One is expected to combat ignorance about information processing technology in those public areas where one's application can be expected to have an adverse social impact.

2.3: Conclusions and Opinions: One is expected to state a conclusion on a subject in one's field only when it can be demonstrated that it has been founded on adequate knowledge. One will state a qualified opinion when expressing a view in an area within one's professional competence but not supported by relevant facts.

2.4: Identification: One shall properly qualify oneself when expressing an opinion outside of one's professional competence in the event that such an opinion could be identified by a third party as expert testimony, or if by inference the opinion can be expected to be used improperly.

2.5: Integrity: One will not knowingly lay claims to competence one does not demonstrably possess.

2.6: Conflict of Interest: One shall act with strict impartiality when purporting to give independent advice. In the event that the advice given is currently or potentially influential to one's personal benefit, full and detailed disclosure of all relevant interests will be made at the time the advice is provided. One will not denigrate the honesty or competence of a fellow professional or a competitor, with intent to gain an unfair advantage.

2.7: Accountability: The degree of professional accountability for results will be dependent on the position held and the type of work performed. For instance:

A senior executive is accountable for the quality of work performed by all individuals the person supervises and for ensuring that recipients of information are fully aware of known limitations in the results provided.

The personal accountability of consultants and technical experts is especially important because of the positions of unique trust inherent in their advisory roles. Consequently, they are accountable for seeing to it that known limitations of their work are fully disclosed, documented, and explained.

2.8: Protection of Privacy: One shall have special regard for the potential effects of computer-based systems on the right of privacy of individuals whether this is within one's own organization, among customers or suppliers, or in relation to the general public.

Because of the privileged capability of computer professionals to gain access to computerized files, especially strong strictures will be applied to those who have used their positions of trust to obtain information from computerized files for their personal gain.

Where it is possible that decisions can be made within a computer-based system which could adversely affect the personal security, work, or career of an individual, the system design shall specifically provide for decision review by a responsible executive who will thus remain accountable and identifiable for that decision.

3. Code of Good Practice

3.1: Education: One has a special responsibility to keep oneself fully aware of developments in information processing technology relevant to one's current professional occupation. One will contribute to the interchange of technical and professional information by encouraging and participating in education activities directed both to fellow professionals and to the public at large. One will do all in one's power to further public understanding of computer systems. One will contribute to the growth of knowledge in the field to the extent that one's expertise, time, and position allow.

3.2: Personal Conduct: Insofar as one's personal and professional activities interact visibly to the same public, one is expected to apply the same high standards of behavior in one's personal life as are demanded in one's professional activities.

3.3: Competence: One shall at all times exercise technical and professional competence at least to the level one claims. One shall not deliberately withhold information in one's possession unless disclosure of that information could harm or seriously affect another party, or unless one is bound by a proper, clearly defined confidential relationship. One shall not deliberately destroy or diminish the value or effectiveness of a computer-based system through acts of commission or omission.

3.4: Statements: One shall not make false or exaggerated statements as to the state of affairs existing or expected regarding any aspect of information technology or the use of computers.

In communicating with lay persons, one shall use general language whenever possible and shall not use technical terms or expressions unless there exist no adequate equivalents in the general language.

3.5: Discretion: One shall exercise maximum discretion in disclosing, or permitting to be disclosed, or using to one's own advantage, any information relating to the affairs of one's present or previous employers or clients.

3.6: Conflict of Interest: One shall not hold, assume, or consciously accept a position in which one's interests conflict or are likely to conflict with one's current duties unless that interest has been disclosed in advance to all parties involved.

3.7: Violations: One is expected to report violations of the Code, testify in ethical proceedings where one has expert or first-hand knowledge, and serve on panels to judge complaints of violations of ethical conduct.

PROCEDURAL REQUIREMENTS FOR REVOCATION OF CERTIFICATE AWARDED

I. A Certification Council, on behalf of the Institute for Certification of Computer Professionals, has the right to revoke any Certificate which has been administered by it in the event that the recipient violates the Codes or engages in conduct which is a discredit or disgrace to the computer profession.

II. The grounds for revocation will be based upon the opinion of at least two-thirds of the members of the Council.

III. Procedure for handling revocation:

1. A formal written statement of charges alleging facts which constitute the grounds for revocation will be prepared.
2. A copy of said charges will be forwarded to the person accused, fixing a time within which such person may file with the Council answers to the charges.
3. If the charges are denied in the answer, the Council will fix a time for the hearing and give notice of the time and place of the hearing to the person accused.
4. Presentation of evidence in support of the charges will be made by the secretary (a non-voting member) of the Certification Council.
5. Presentation of evidence in defense of the charges will be made by the accused or the designated representative of the accused.
6. Ample opportunity for both sides to present facts and arguments will be allowed at the hearing.
7. At the conclusion of the hearing, the Council will determine whether or not the charges have been sufficiently established by the evidence and whether the Certificate should be revoked or should not be revoked.
8. The accused will be notified of the decision by registered mail.
9. The accused has the right to request review of the decision by the Executive Committee of ICCP, provided an appeal in writing is submitted to the President, ICCP, within 30 days of the accused's receipt of the Council's decision.

Enforcement procedures for the DPMA Code of Ethics and Standards of Conduct approved

The following includes documents approved at the 1981 and 1982 Data Processing Management Association International Board of Directors meetings. The enforcement procedures take effect Jan. 1, 1983. DPMA has long been involved in the establishment of ethics and standards within the profession. The ID action taken in Chicago (see article, this section) is an evolution of that commitment.—Ed.

Code of Ethics

I acknowledge:

That I have an obligation to management, therefore, I shall promote the understanding of information processing methods and procedures to management using every resource at my command.

That I have an obligation to my fellow members, therefore, I shall uphold the high ideals of DPMA as outlined in its International Bylaws. Further, I shall cooperate with my fellow members and shall treat them with honesty and respect at all times.

That I have an obligation to society and will participate to the best of my ability in the dissemination of knowledge pertaining to the general development and understanding of information processing. Further, I shall not use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to me or to which I may gain access.

That I have an obligation to my employer whose trust I hold, therefore, I shall endeavor to discharge this obligation to the best of my ability, to guard my employer's interests, and to advise him or her wisely and honestly.

That I have an obligation to my country, therefore, in my personal, business and social contacts, I shall uphold my nation and shall honor the chosen way of life of my fellow citizens.

I accept these obligations as a personal responsibility and as a member of this association. I shall actively discharge these obligations and I dedicate myself to that end.

Standards of Conduct

These standards expand on the Code of Ethics by providing specific statements of behavior in support of each element of the Code. They are not objectives to be strived for, they are rules that no true professional will violate. It is first of all expected that information processing professionals will abide by the appropriate laws of their country and community. The following standards address tenets that apply to the profession.

IN RECOGNITION OF MY OBLIGATION TO MANAGEMENT I SHALL:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

IN RECOGNITION OF MY OBLIGATION TO MY FELLOW MEMBERS AND THE PROFESSION I SHALL:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

IN RECOGNITION OF MY OBLIGATION TO SOCIETY I SHALL:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect and abide by the appropriate local, state, provincial and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

IN RECOGNITION OF MY OBLIGATION TO MY EMPLOYER I SHALL:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Enforcement Procedures

1. Filing a Complaint

1.1 Any complaint against any Regular or Honorary Member of the Association shall be in writing, signed by the complainant, properly notarized and submitted by certified or registered mail to the Executive Director at International Headquarters. At a minimum, the complaint must include:

1.1.1 a concise statement of the facts on which the complaint is based;

1.1.2 citations to the section of the Code of Ethics and Standards of Conduct that were allegedly violated;

1.1.3 a statement that the facts are true to the best of the complainant's knowledge and belief;

1.1.4 a statement that the complainant is willing to appear at the expense of DPMA at a hearing with the accused, if requested.

1.2 Charges may be initiated only by a Regular or Honorary member in good standing of the Association.

1.3 If the accused is a Chapter president or an Individual member the complaint will

DPMA Enforcement Procedures

be referred to the International President.

2. Initial Action

2.1 The complaint shall be immediately reviewed by the Executive Director to determine whether it complies with Section 1. If the complaint is defective in any respect, International shall return it to the complainant with a letter citing the deficiency and a copy of these Rules and Regulations.

2.2 Notification of complaints that meet the requirements of Section 1 shall be forwarded with all documentation to the Chapter President, Chapter International Director, Region Vice President, and the International President within 10 days.

2.3 The Chapter President or International President shall appoint a Hearing Committee composed of not less than four members of the Chapter, or the Executive Council, as appropriate, and chaired by the Executive Vice President or appropriate Chapter/International Officer to perform the functions specified in these procedures. No member of this committee can be directly involved in the complaint in any way. The Region Vice President shall appoint a Region Hearing Committee representative to be included as a voting member of the Hearing Committee. The representative must be a member of the Region but not from the Chapter involved.

3. Preliminary Determination

3.1 The Hearing Committee shall within 10 days send the person against whom allegations have been made, hereafter known as the respondent, a copy of the complaint and these Rules and Regulations by certified or registered mail to be delivered to addressee only, return receipt requested, or by personal delivery to the respondent.

3.2 The notification to the respondent will inform him or her that he/she may file a written reply to the Hearing Committee within 60 days of receipt of the complaint. The respondent shall be further notified that, if he/she fails to file a response, the action against him/her will proceed. The Hearing Committee will make a minimum of two attempts to contact the respondent before continuing the process. Failure to respond will not be taken as proof of guilt. The Hearing Committee will proceed with facts available to them.

3.3 The respondent may elect to refute the allegation. This refutation should directly address the facts alleged in the complaint and must state that the response is true to the best of his/her knowledge and belief.

3.4 A copy of the response shall be sent by the Hearing Committee to the complainant.

3.5 Upon receipt of the response, the Hearing Committee shall, within 30 days, determine whether to dismiss the complaint as unworthy of further consideration or proceed with formal hearing.

3.6 The complainant and the respondent shall be notified of the Hearing Committee's preliminary determination by certified or registered mail within 10 days of the action.

3.7 There shall be no right to appeal the preliminary determination of the Hearing Committee.

3.8 All documentation concerning the case will be returned to International for retention and protection as covered in Section 11. In the case of a dismissed or withdrawn complaint, all documentation shall be sealed and returned to the International Executive Director. The Chapter President, Chapter International Director, Region Vice President, and International President shall be notified of the disposition of the complaint.

4. The Hearing

4.1 At its discretion, the Hearing Committee will interview the complainant, the respondent, and other individuals who have knowledge of the facts alleged. The International Association shall bear the expense of travel, lodging and meals for such interviews. The complainant and the respondent may have access to information obtained in these interviews.

4.2 The Chairperson shall prescribe any procedures for the hearing not consistent with the provisions of this section.

4.3 After a complaint has reached the formal hearing stage, it may be withdrawn by the complainant only with the Hearing Committee's approval.

4.4 The complainant or respondent may be represented by legal counsel. If the Hearing Committee desires, legal counsel for the International Association may give assistance by way of counsel or participation in the proceedings of any hearing or by way of counsel at times other than hearings.

4.5 A transcript of the hearing will be made by DPMA. Participants in the hearing may have access to the transcript. DPMA will pay for the cost of transcripts for the complainant and respondent and will provide them at reproduction cost to other participants if requested.

4.6 The Hearing Committee shall appoint a time and place for the hearing of the complaint and shall notify the complainant and respondent personally or by certified or registered mail at least 60 days before the hearing. Depositions are acceptable in the event that individuals cannot appear at the hearing.

4.7 The Hearing Committee shall be the sole judge as to the character of evidence to be received and the procedures to be followed. Parties, their legal counsel (if any), counsel for the International Association, or any member of the Hearing Committee may question and cross-examine any witness.

4.8 The Hearing Committee may adjourn the hearing from time to time as, in its judgment, justice or expediency requires.

4.9 The specific witness to be called shall be at the discretion of the Hearing Committee. DPMA will pay for travel, lodging, and meals for these witnesses, if necessary. Witnesses called beyond those scheduled by the Hearing Committee will be at the expense of the interested party.

4.10 When any member of the Association receives written notification from the Hearing Committee, the complainant or the respondent, to appear and testify as a witness at such hearing, it shall be the member's duty to testify or to submit a properly notarized affidavit.

4.11 Members appointed to a Hearing Committee shall serve until the matter is disposed of. Committee members who shall resign or be discharged for whatever reason shall be replaced under the same conditions as in 2.3 above.

5. Decision of the Hearing Committee

5.1 The decision of the Hearing Committee shall be rendered within 60 days of the hearing and shall be by two-thirds affirmative vote of the committee members present. It shall be in writing and contain findings of fact and a statement of the recommended disciplinary action, if any.

5.2 The decision concerning the respondent shall be:

5.2.1 to dismiss the complaint; in which case all records of the proceedings will be sealed and returned to the International Executive Director.

5.2.2 to censure; in which case a letter of censure will be written to the respondent.

5.2.3 to suspend; in which case all privilege of membership will be revoked.

5.2.4 to expel; in which case the privilege of membership will be revoked.

5.2.5 Adverse action (5.2.2, 5.2.3 and 5.2.4) will be taken only after the process of appeal has been exhausted.

5.3 The Hearing Committee, in its sole discretion, may also reopen the hearing within 30 days of the first hearing for additional evidence to be provided either in person or in writing. Such action would not extend the rendering of the decision for more than 30 days.

5.4 In the event the respondent is found in violation, the Committee may, in its discretion, consider in determining discipline all past records in the DPMA file of previous, relevant determinations of violations.

5.5 The Chairperson shall, within 10 days, send a copy of the decision to the

DATA MANAGEMENT

39-741 O - 84 - 8

International Headquarters' Corporate Operations Committee and to the International Legal Counsel for their review for consistency with the DPMA bylaws. They shall have 10 days to accomplish their review.

5.6 After their review, the Chairperson shall, within 10 days, submit copies of the decision to the complainant and the respondent by certified or registered mail. If the decision is adverse to the respondent (i.e., censure, suspend, expel), he/she shall have 30 days from the time that the Notice of Decision is received to file a Notice of Appeal.

6. The Appeals Committee

6.1 The International President shall appoint an Appeals Committee of not less than three members of the Executive Council to hear the case on appeal provided that no person:

6.1.1 who has been involved in the facts underlying the complaint;

6.1.2 who is a member of the Region involved; or

6.1.3 who is a member of the Hearing Committee

may hear the same case on appeal.

6.2 Appeals may be taken to the Appeals Committee only from decisions of the Hearing Committee adverse to the respondent.

6.3 If Notice of Appeal is not filed within 30 days of the receipt of the Notice of Decision, the decision of the Hearing Committee shall become final, binding and effective at the beginning of the day after the appeal could have been properly filed.

7. The Appeal Process

7.1 The Notice of Appeal must be in writing, signed by the appellant and contain a statement with sufficient specificity and argument to set forth the grounds upon which the appeal is taken. It shall be sent to the International President by certified or registered mail, and must include the reasons why the decision of the Hearing Committee should be modified, reversed or remanded for further proceedings. Only those arguments advanced in the written Notice of Appeal shall be allowed to be presented to the Appeals Committee at its hearing, except for good cause shown as to why the Appeals Committee should allow additional oral argument.

7.2 The International President shall send a copy of the Notice of Appeal to all members of the Hearing Committee and the Appeals Committee, the Executive Director, legal counsel for the International Association, and to all parties. If within 20 days after receipt of the Notice of Appeal, the International President and the Chairperson of the Hearing Committee, after consultation with legal counsel, agree, the appeal may be stayed pending further action by the Hearing Committee relative to the matters raised in the Notice of Appeal. In such event, all parties shall be notified of the action by certified mail. The Hearing Committee shall take such action as may be necessary to cure any procedural matter raised, including, but not limited to, rehearing the matter. If the appeal is not stayed by such action, the appeal will proceed to hearing in accordance with these Rules and Regulations.

8. Procedures for Hearing the Appeal

8.1 The Appeals Committee shall hear the appeal within 30 days from the date that the Notice of Appeal is issued unless stayed as in Section 7.

8.2 Copies of the Notice of Appeal, supporting materials, and written transcript and exhibits, if any, shall be presented in advance of the meeting to sitting members of the Appeals Committee.

8.3 The International President shall serve as Chairperson of the Appeals Committee. In his/her absence, he/she may designate any other member of the Executive Council to serve as Chairperson consistent with Section 6.1.

8.4 The parties to the appeal may be represented by legal counsel. The services of the International Legal Counsel shall be available to the Appeals Committee.

8.5 The Chairperson shall determine whether a quorum is present and, if so, shall convene the meeting at the time set. If a quorum is not present, the Chairperson may adjourn the hearing until such time as a quorum is present. A quorum shall be a majority (i.e., more than half) of the members of the Appeals Committee.

8.6 The Chairperson shall introduce each person present at the meeting and give the parties the opportunity to challenge the participation of any Appeals Committee member present.

8.7 If objection is raised and the individual challenged chooses not to withdraw, the Chairperson, in his/her discretion, may determine whether the person objected to should participate further in the proceedings.

8.8 The Chairperson may dismiss any person from the meeting who fails to conduct himself/herself in a manner conducive to a fair and expeditious hearing of the appeal.

8.9 Each party to the appeal shall have a maximum period of 20 minutes to initially present his/her case to the Appeals Committee.

8.10 The Chairperson shall not permit any additional evidence to be presented to the Appeals Committee. No written evidentiary material may be presented to the Appeals Committee unless such material was presented to the Hearing Committee at the time of its deliberations.

8.11 A representative of the Hearing Committee shall proceed first by presenting a summary of the case and the reasons for the Hearing Committee's decision.

8.12 Members of the Appeals Committee and the International Legal Counsel shall have the opportunity to question the representative of the Hearing Committee.

8.13 The appellee shall have the right to state his/her position as to why the decision should be upheld.

8.14 Members of the Appeals Committee and the International Legal Counsel shall have the opportunity to question the appellee.

8.15 The appellant, or his/her counsel, shall then present his/her case to the Appeals Committee, stating specifically why the decision should be modified, reversed, or remanded.

8.16 Members of the Appeals Committee and the International Legal Counsel shall have the opportunity to question the appellant.

8.17 Each party shall have the opportunity to summarize his/her position.

8.17.1 The representative of the Hearing Committee shall have 10 minutes to summarize the Hearing Committee's position and to rebut any statement made by the appellant.

8.17.2 The appellee shall have 10 minutes to summarize his/her position and to rebut any statement made by the appellant.

8.17.3 The appellant shall have 10 minutes to summarize his/her position and to rebut any statements made by the appellee or by the representative of the Hearing Committee.

8.18 Appeals Committee members and the International Legal Counsel shall have a final opportunity to question the parties.

8.19 The Chairperson shall dismiss the parties and recess the Appeals Committee meeting.

8.20 The Appeals Committee may, in its sole discretion, alter or waive any procedural requirements, including time limitations except that each party must be granted a minimum of 10 minutes to summarize his/her position as in Section 8.17.

9. Appeals Committee Deliberation

9.1 The Chairperson shall immediately reconvene the Appeals Committee in Executive Session for the purpose of rendering a decision on the appeal.

9.2 The Chairperson shall permit each Appeals Committee member to discuss his/her views on the disposition of the appeal. International Legal Counsel, the Executive Director or his/her designee may also attend such session. They will be present to offer advice and counsel if called upon to do so.

DPMA Enforcement Procedures

9.3 The Appeals Committee's review shall be limited to the review of the action of the Hearing Committee and the determination of whether the action has been proper or if procedural error has been committed by the Hearing Committee.

9.4 The Appeals Committee shall, by two-thirds affirmative vote of members present, affirm, reject, or modify the decision of the Hearing Committee, or shall request the Hearing Committee to take further action, including, but not limited to, rehearing the case.

9.5 The decision of the Appeals Committee shall be final and binding. Each member of the Association by becoming, or continuing as a member, agrees not to seek review of the decision of either the Hearing Committee, or the Appeals Committee in any court of law or equity or by any governmental body.

10. Notification of Decisions

10.1 The Chairperson of the Hearing or Appeals Committee shall, by certified or registered mail, notify the appellant, the complainant, and the Hearing Committee of the decision of the Appeals Committee within 10 days of the decision.

10.2 Final decisions will be sent to all participants in the hearing and/or appeal process within 10 days after all possible avenues of appeal have been exhausted. The Hearing and/or Appeals Committee will prepare a summary of the case that discusses the situation, the findings, and the reasons for the findings. There shall be no reference to any of the individuals or organizations involved by name. These summaries will be published in DATA MANAGEMENT Magazine for educational purposes and to create a body of knowledge of ethical behavior and to support the refinement of the Code, Standards and procedures.

10.3 All formal actions taken on the appeal by the Appeals Committee shall be made a matter of record in its minutes.

10.4 The Appeals Committee shall also notify the Executive Council of its decision.

11. Record Retention and Availability

11.1 The International office shall maintain a record of all Hearing Committee formal action received and all documentation pertaining to each case. In the event that a determination to take no action is made, the records will be sealed and may be used only in accordance with these regulations. Records of cases which shall have been dismissed shall be maintained only for a period of seven years from the date of dismissal and shall thereafter be destroyed by the International Executive Director.

11.2 The records of the Hearing Committee and the Appeals Committee on a particular case and all pertinent documentation relating thereto shall be retained by the International Association.

11.3 Requests for information on a specific case must be in writing and signed by the person making the request. Information may be released if the Corporate Operations Committee and the original parties, if not deceased, approve such release in advance in writing.

11.4 Requests for general information on ethical proceedings may be responded to by release of statistical information prepared by the staff, provided that the approval of the Corporate Operations Committee is obtained in advance.

"What can DPMA do for you?
MAP is a good answer to that question!"

J. Max Hoffmann, member,
Cornhusker Chapter
Lincoln, Nebraska
MAP Facilitator - Region 4

project MAP:

The DPMA Management Assistance Program

— **MAP** is a time and cost effective method of management development and training.

— **MAP** is not only a great educational tool, but an income producer for many chapters.

— **MAP** relates directly to each participant's current work situation.

— **MAP** is designed to be of value to all participants, regardless of previous management training or experience.

More than 100 MAP workshops have been conducted or scheduled so far in 1982, and more are being scheduled each day.

Contact your chapter education chairperson to schedule a MAP workshop.

Mr. GLICKMAN. Our last witness is Mr. Joseph B. Tompkins, chairman, Task Force on Computer Crime, with the American Bar Association.

We appreciate your being here. I would tell you, we save the best till last, to make you feel good.

Mr. TOMPKINS. I'm glad you said that. Thank you.

Mr. GLICKMAN. OK. Go ahead and proceed.

STATEMENT OF JOSEPH B. TOMPKINS, JR., CHAIRMAN, TASK FORCE ON COMPUTER CRIME, AMERICAN BAR ASSOCIATION

Mr. TOMPKINS. Mr. Chairman, it's a pleasure to be here today on behalf of the American Bar Association and its Criminal Justice Section's Task Force on Computer Crime.

I have prepared a statement which I would assume will be part of the record of this hearing, and if it's agreeable to you, I will briefly summarize the contents of that statement.

In June of this year, our Task Force on Computer Crime, which is part of the Criminal Justice Section of the American Bar Association, published a report on computer crime. The report was prepared on the basis of a nationwide survey that our task force did.

Our task force is part of the White Collar Crime Committee. We—as background to our report in the survey, the American Bar Association in 1979 did some extensive work on computer crime and in fact proposed a resolution that was passed by the House of Delegates in the American Bar Association, but not a lot of work had been done since that time.

So it occurred to us it was time to look back and see what had changed since 1979 when the American Bar Association came out in favor of Federal computer crime legislation, and we began to look at the available writings and the evidence, and we found that there was not a great deal of useful empirical evidence concerning the nature and extent of computer crime. So that was part of the reason behind the survey that we did.

The survey was sent to approximately 1,000 private organizations and government agencies, including the Fortune 500 companies, banks, insurance companies, financial services, brokerage firms, accounting firms, all major Federal departments and agencies, all State attorneys general, and a sample of district attorneys.

The survey contained questions eliciting information in a number of different areas—the nature and importance of computer crime, the effects of computer crime, the perpetrators of computer crime, prevention and deterrence of computer crime, and other related information.

We received responses to the survey from 283 organizations. The respondents were a cross-section of large private and public agencies. They included a sampling from each of the groups that I mentioned. They also included 13 Federal agencies and 28 State or local law enforcement agencies.

The complete survey results are contained in the report on computer crime which was published in June and is available from the American Bar Association here. I would just highlight a few of the more significant results from the survey.

The survey respondents were asked to identify the "known and verifiable types of incidents of computer crime" experienced by their organizations during the last 12 months.

Two hundred and thirty-seven respondents answered the inquiry, and, of that, 136 indicated that they had experienced known and verifiable incidents of computer crime during the last 12 months. That amounted to approximately 48 percent of the total number of respondents to the survey.

The most frequently mentioned incidents of computer crime were unauthorized use of computers for personal programming activities, theft of computer software, use of computers to steal tangible and intangible assets, and theft of computer hardware.

The survey respondents were then asked if they could quantify the known and verifiable losses they had experienced during the last 12 months.

In response to that question, 27 percent of the respondents were able to quantify their losses; 28 percent said they were not in a position to quantify their losses—they either had no system to monitor losses or no available estimate of losses; and 45 percent indicated they had no losses—known and verifiable losses during the last 12 months.

We point out in our report that it seems significant to us that 27 percent of those responding were able to quantify known and verifiable losses, and of this relatively small group—it amounts to 72 organizations, private and public—the annual losses for that group alone could be anywhere from $145 million to $730 million.

The range is that large because in the survey we had brackets of dollar amounts that the respondents could check—$0–$100,000; $100,000–$500,000—and to come up with a range, we took the minimum amount in each bracket and added it and the maximum amount in each bracket, and that's how we came up with the $145 million to $730 million, which, if you look at a per respondent average annual loss figure, amounts to between $2 million and $10 million per respondent reporting losses.

On the basis of that and other information available to us, we concluded in that report that the annual losses sustained by American business and government as a result of computer crime are, by any measure, huge.

We made it clear in our report that we are not in a position to quantify what the total national losses are due to computer crime, and we don't think at this point anyone is, given the lack of adequate reporting systems and data collecting systems.

Our conclusions were based simply on the results from this relatively small sample group.

We asked other questions concerning the perpetrators of computer crime, of known incidents of computer crime, and our survey results indicated that more respondents indicated that the perpetrators were individuals within the organization than individuals outside the organization, and, in a significant number of incidents, the perpetrator was never identified.

Those findings seem to confirm the views of many commentators both that computer crime is more likely to be committed by an insider than an outsider and that in many cases we don't know who the perpetrator is.

The survey results also indicated that roughly one-third of the respondents who had experienced computer crime had reported none of the incidents to law enforcement authorities, and another third had reported only some of the incidents; 16 percent had reported all of the suspected incidents.

Another result that I will just touch on briefly—we asked the respondents for their views regarding the need for a Federal criminal statute directed specifically at computer crime. Fifty-eight percent strongly supported such a statute. Twenty-one percent somewhat supported such a statute.

It was significant to us that 79 percent of those surveyed supported a Federal statute either strongly or in some degree.

We had a question in the survey which allowed the respondents in their own words to describe what they consider to be the most troublesome aspect of computer crime currently and in the foreseeable future.

Over 60 percent of the respondents chose to answer that question and provided their own handwritten comments. We have categorized those into the most frequently mentioned categories.

The most frequently mentioned item, the most troublesome item, was proliferation of business and personal computers and computer users. Second—the second most frequently mentioned item was the difficulty in detecting computer crime. The third most mentioned item was the vulnerability or lack of adequate security measures to prevent or deter computer crime; and fourth was the lack of public and/or managerial awareness and concern.

These comments, to us, seem to summarize both in their tone and in their content the depth of concern among those who responded to our survey, and as I indicated in my statement, we are making all those comments available to the subcommittee as an appendix to my statement.

The findings of our report, although we were looking at somewhat different issues, support a number of the findings that were made by this subcommittee in its April 1984, report. Among those are—in this subcommittee's report there was a finding that there is a need for effective and low-cost computer communications safeguards and that appropriate technological protective measures do not exist for all applications.

In our report, we indicate that the comments from the survey respondents repeatedly indicated a concern regarding the lack of effective computer security technology as well as a lack of sufficient management concern regarding computer security problems. This supports the subcommittee's finding in that regard.

Second, this subcommittee in its report found that, while media attention focuses on the threat of computer hackers and other outside intruders, the greatest threat to computerized resources remains personnel who are authorized to access them.

The survey responses that we received tend to support that, as I indicated a few minutes ago, although there are recent incidents of computer hacking by outsiders which cause us great concern.

Third, the subcommittee found in its report that there is a shortage of capable and well trained computer security personnel. The responses to our survey indicated that both private industry and public officials believe that law enforcement personnel do not have

the expertise necessary to investigate and prosecute computer crime successfully.

Finally, the subcommittee report noted that the lack of reliable statistics on computer and communications systems abuses contributes to a misunderstanding of the problem and hampers implementation of adequate safeguards. The work of our task force indicates that the subcommittee finding in this respect is correct. In both the private and the public sectors, there is a remarkable lack of knowledge concerning both the nature and extent of computer crime.

In closing, I would note that in 1979 in its resolution, the American Bar Association endorsed the need for adoption of Federal computer crime legislation. The results of our survey and our report indicate that the need, if it existed in 1979, is even more compelling now, for a number of reasons.

The existence of a Federal computer crime statute directed at computer-related illegal activity would dispel the perception which apparently is shared by a significant portion of the population that computer abuse is a game that one may engage in freely without fear of prosecution.

As Federal computer crime statute should also aid law enforcement efforts generally by providing investigators and prosecutors a clear and specific jurisdictional hook and a framework for prosecution.

Third, Federal computer crime legislation should make the sanctions for committing computer crime more rational and more consistent with the seriousness of the crime.

Fourth, a Federal computer crime statute should assist the Federal Government in protecting itself and the public at large against the potentially devastating effects of manipulation or destruction of the Government's own computers.

And, fifth, the passage of a Federal computer crime statute is also likely to enhance the collection of meaningful data concerning the occurrence and nature of computer crime.

For those and other reasons, the American Bar Association in 1979 and today strongly supports the passage of Federal computer crime legislation.

Our task force is now in the process of reviewing some of the pending Federal legislation and also existing State legislation which, according to my figures, now exists in 31 separate States.

Finally, I would just point to an incident that occurred less than 2 weeks after our report came out in June, and that is the TRW incident, and I point to it not to make any specific reference to TRW or anyone else but just as an example that illustrates the vulnerability that we have as private citizens, and as businesses, and as Government agencies to computer crime.

As you may recall, as it was reported in the press, the TRW incident involved the credit histories of 90 million people that were contained in the computer files of TRW information systems.

Based on press reports, it appears that the TRW computerized credit files are accessible by retail stores and other subscribers by means of a password.

The password to that databank with 90 million people's credit card records was obtained improperly from someone at a Sears, Roebuck store on the west coast. The password was then posted on

an electronic bulletin board, which made it available to all of the bulletin board subscribers.

Once the password was obtained, a computer user could use it along with publicly available information, such as a credit card holder's name, address, and date of birth, to obtain numbers of all credit cards owned by the card holder as well as other credit information, such as credit limits. This information, in turn, could be used to charge merchandise to the card holder's credit cards.

According to a spokesman for TRW, the password could have been illegally used anywhere from a week up to a month before they discovered the breach and changed the password.

TRW reported there was no "unusual activity" involving the use of that password during the relevant period, but they also acknowledged that there is no way to determine who used the password during that period, what information was improperly obtained from the databank, and what use was made of that improperly obtained information.

The extent of improper use, if it's ever known, may only be known if the 90-million credit card holders notice and report improper or unauthorized charges appearing on their credit card statements, and, even then, tracing the charges back to the breach of TRW's computers may be impossible; and, finally, and I think importantly, it should be noted that TRW found out about the improper infiltration only because of a tip from an informant.

The TRW incident and other incidents like it raise serious questions about the adequacy of the laws that we have now and also the adequacy of existing computer security.

The TRW incident, along with the responses to our survey, indicate how difficult it is to prevent computer crime in the first place, how difficult it is to detect it once it has occurred, how difficult it is to investigate and prosecute it if and when it is detected.

In closing, I would just like to indicate the American Bar Association's support for the subcommittee's efforts. For our part, our task force and others in the American Bar Association intend to continue to study computer crime to attempt to contribute to the public debate on the subject and to recommend specific steps that we feel should be taken by both the public and private sectors to minimize and prevent the occurrence of computer crime.

Thank you, Mr. Chairman. I'd be glad to answer any questions.

Mr. GLICKMAN. Thank you.

Are you aware of some of the computer crime bills that have passed out of the House at least this year, in the last 3 months or so?

Mr. TOMPKINS. I am aware of several of those. The ones that seem to be the most prominent that I'm aware of are H.R. 5616, which I think the House has passed.

Mr. GLICKMAN. That's the Hughes bill on——

Mr. TOMPKINS. That's the Hughes bill. And on the Senate side, S. 2940, which I think is the administration's bill, introduced by Senator Thurmond.

Mr. GLICKMAN. Did you take any specific position on either of those bills?

Mr. TOMPKINS. No, we have not. Those are among the pieces of legislation that we're looking at.

Mr. GLICKMAN. During your survey, were you able to characterize the attitude of upper management toward computer crime? That is, you've got some high numbers on some of these questions, but as far as you are aware, did they really care about the problems? Was it a serious problem to them, do you think?

Mr. TOMPKINS. I think it's hard to get any specific read on—on that. What did come through—and it came through largely in the comments that I mentioned that are part of the appendix to my statement—is a feeling on the part of those who deal with computers directly on a daily basis—the computer operators—that their own management is not concerned enough about computer security, and either because their efforts have not been successful or because of a lack of understanding on management's part, there's not enough attention placed upon computer security, and there may be an underinvestment in computer security.

I think also there was an indication that there is a gap in technology—that is, a gap between the technology of computer use and application and the technology of computer security.

What came through a number of the comments is that in developing computer systems, the emphasis is on, how can we extend the use and application of the computers, and then almost as an afterthought there is some attention given to computer security.

Mr. GLICKMAN. What is the worst example of computer crime that you found?

Mr. TOMPKINS. In our survey, we did not ask people to describe in detail each incident of computer crime that they had experienced, and we did not ask them to identify the modus operandi or how it had occurred.

In terms of amount of economic losses, one of the survey respondents indicated known and verifiable economic losses of between $100 and $500 million in 1 year.

Mr. GLICKMAN. I think you indicated that—you made some statement that losses are huge. Did you not say that in the aggregate sense?

Mr. TOMPKINS. Our conclusion, based on what we found in the survey, was, we think the losses among the 72 respondents who indicated that they had known losses, are substantial, significant, and looking at that small group, if that's the kind of losses that they have experienced, we have no problem in concluding that the losses nationwide are huge.

Mr. GLICKMAN. OK. Well, thank you very much for your testimony today. We appreciate it.

Mr. TOMPKINS. Thank you.

Mr. GLICKMAN. This concludes the hearing this afternoon.

[Whereupon, at 3:50 p.m., the subcommittee was adjourned.]

[The prepared statement of Mr. Tompkins follows:]

AMERICAN BAR ASSOCIATION

GOVERNMENTAL AFFAIRS GROUP • 1800 M STREET, N.W. • WASHINGTON, D.C. 20036 • (202) 331-2200

STATEMENT

OF

JOSEPH B. TOMPKINS, JR.

CHAIRMAN
TASK FORCE ON COMPUTER CRIME
SECTION OF CRIMINAL JUSTICE
AMERICAN BAR ASSOCIATION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION
AND MATERIALS
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

September 24, 1984

Mr. Chairman and Members of the Subcommittee, I am very pleased to be here today, on behalf of the American Bar Association and its Criminal Justice Section's Task Force on Computer Crime, to participate in your inquiry concerning computer and communications security and privacy. As you may know, in June of this year, our Task Force published a Report on Computer Crime, presenting the results of a nationwide survey we conducted concerning computer-related crime and analyzing the significance of those results in the context of other information available to us and the American Bar Association's existing policy with respect to the need for federal computer crime legislation.*/ Today, I would like to review briefly some of the findings of our Report and then discuss the significance of those findings in light of this Subcommittee's April 1984 Report on Computer and Communications Security and Privacy and recent developments in the area of computer crime. I will be glad to respond to any questions you may have during or at the end of my statement.

I. THE ABA TASK FORCE REPORT ON COMPUTER CRIME

In February 1984, our Task Force distributed a lengthy survey to approximately 1,000 private organizations and public

---

*/ The members of the Task Force are Joseph B. Tompkins, Jr., Chairman (Sidley & Austin, Washington, D.C.); Judge James R. Jorgenson (Third District Court of Appeals, Miami, Florida); Nathaniel E. Kossack (Perito, Duerk & Pinco, Washington, D.C.); and Marcia L. Proctor (State Board of Law Examiners, St. Paul, Minnesota).

agencies, including the Fortune 500 companies, banks, insurance companies, financial services/brokerage firms, accounting firms, all major federal departments and agencies, all state attorneys general and a sample of district attorneys. The survey contained questions eliciting information in a number of different areas -- the nature and importance of computer crime, the effects of computer crime, the perpetrators of computer crime, prevention/deterrence of computer crime, and information concerning the responding organizations and the basis for their responses to the survey.

Two hundred eighty-three (283) organizations responded to the survey. The respondents represented a cross-section of large private and public agencies, with the largest categories of respondents being manufacturers of equipment and materials (44), State/local law enforcement agencies (28), producers of consumer goods (27), computer/electronics firms (27), conglomerates (20), insurance companies (17), and banks (16). Our survey respondents also included thirteen (13) federal agencies. Forty-eight (48) percent of the respondents reported annual revenues (or budgets) of over $1 billion, and forty-four (44) percent employed 10,000 or more employees. The survey respondents were geographically diverse, with the largest number being located in the Northeast (33%) or North Central (30%) United States.

The complete survey results are contained in our Report on Computer Crime, but I would like to highlight here a few of the more significant results.

A. Incidence of Computer Crime/Economic Losses

The survey respondents were asked to identify the "known and verifiable types of incidents of computer crime" experienced by their organizations during the last twelve months. Two hundred thirty-seven (237) respondents answered this inquiry; of this group, one hundred thirty-six (136) respondents indicated that they had experienced known and verifiable incidents of computer crime during the last twelve months. This amounts to approximately 48% of the total number of respondents (283).

The most-frequently-mentioned incidents of computer crime were as follows: 1) unauthorized use of computers for personal programming activities (63); 2) theft of computer software (45); 3) use of computers to steal tangible or intangible assets (44); and 4) theft of computer hardware (43). The least-frequently-mentioned incidents of computer crime were: 1) use of computers to commit sabotage (13); 2) destruction of computer hardware (10); 3) theft of coded output data (7); and 4) use of computers to perpetrate extortion or blackmail (5).

The survey respondents were then asked to indicate "known and verifiable losses due to computer crime experienced during the last twelve months." The results are as follows:

Table 1

Known and Verifiable Losses Due to Computer Crime Experienced During the Last Twelve Months

Amount	Number of respondents	Percentage of total
None	125	45%
Between 0 and $100,000	54	20
Between $100,000 and $500,000	8	3
Between $500,000 and $1 million	1	-
Between $1 million and $5 million	4	2
Between $5 million and $10 million	0	-
Between $10 million and $50 million	4	2
Between $50 million and $100 million	0	-
Between $100 million and $500 million	1	-
Over $500 million	0	-
No available system to monitor losses	41	15
No available estimate of value of losses	37	13
Total number of responses	275	100%

As we stated in our Report, one cannot extrapolate from the results of this limited survey to derive a valid "total annual dollar loss" figure for computer crime, a figure which is unattainable given the current state of record keeping. Nonetheless, it does appear significant, given the conservative manner in which the survey question was framed, that 27% of those responding have sustained "known and verifiable losses due to computer crime during the last twelve months," and that the annual losses for this small group of respondents could range anywhere from $145 million to as high as $730 million. That

translates to an average annual loss per respondent reporting losses of between $2 million and $10 million.*/

Based on these and other responses to our survey, we concluded that "the annual losses sustained by American business and government organizations as a result of computer crime are, by any measure, huge." While none of us is in a position to put even an approximate price tag on the annual costs of computer crime, such a quantification of aggregate losses should not be necessary to convince any of us that computer crime is a problem of substantial and growing significance.

B. Perpetrators of Computer Crime/Reporting to Authorities

The survey respondents were asked a series of questions concerning the identity and motivation of perpetrators of known incidents of computer crime. Of the two hundred sixty-five (265) respondents replying to the question concerning the identity of perpetrators, one hundred sixty (160) indicated that the question was applicable to them. Their responses were as follows (multiple responses were permitted):

---

*/ The survey results indicated a somewhat higher incidence of known and verifiable losses for larger businesses (annual revenues over $1 billion) than for smaller businesses (annual revenues under $1 billion), but the difference was not substantial.

Table 2

Identity of Perpetrators of Known Incidents of Computer Crime

Response		Number of respondents	Percentage of respondents (160)
Perpertrator not identified		62	39%
Individuals within the organization		125	77
a. Executives, managers not directly involved with computers	21		
b. Computer operations supervisors	22		
c. Computer programmers, software personnel	67		
d. Nonsupervisory computer operations personnel	42		
e. Nonsupervisory personnel not directly involved with computers	40		
f. Other	18		
Individuals outside the organization		73	45
a. Competitors	16		
b. Customers/clients	11		
c. Outside consultants	22		
d. Individuals with no prior relationship with organization	37		
e. Other	16		

(Total number of respondents = 160)

These results seem to confirm the views of many that computer crime is more likely to be committed by an insider than an outsider and that a large portion of computer crime perpetrators are never identified.

The respondents were then asked to indicate the extent to which they had reported incidents of computer crime, and suspected perpetrators, to law enforcement authorities. Their responses were as follows:

Table 3

Reporting Computer Crime Incidents to Law Enforcement Authorities

	Number of respondents	Percentage of total
All such incidents reported	40	16%
Most such incidents reported	13	5
Some such incidents reported	45	18
None of such incidents reported	50	20
Not applicable	102	41
Total number of responses	250	100%

It appeared significant to us that, of the respondents to whom the above question was applicable, approximately one-third did not report any of the computer crime incidents experienced to law enforcement authorities, and another one-third only reported some of the incidents experienced.

C. Prevention and Deterrence of Computer Crime/Need for Federal Legislation

The respondents to our survey were asked several questions concerning the prevention and deterrence of computer-related crime. They were first asked to review a list of various means of preventing and deterring computer crime and then to rank

the alternatives in terms of effectiveness (a rank of one (1) indicates the most effective, two (2) indicates the next most effective, and so on). The resulting ranking was as follows:

Table 4

Most Effective Means of
Preventing and Deterring Computer Crime

Action	Number of respondents	Relative Score(Rank)
More comprehensive and effective self-protection by private business	246	1.53
Education of users concerning vulnerabilities of computer usage	210	2.78
More severe penalties in federal and state criminal statutes	193	3.62
Greater education of the public regarding computer crime	168	4.07
More aggressive federal law enforcement	166	4.13
More aggressive state and local law enforcement	174	4.17
Greater caution by individual consumers, investors, entrepreneurs	163	4.38
(Total number of respondents = 259)		

The respondents were then asked to identify the steps that their organizations have in fact taken to prevent and deter computer crime. Their responses were as follows (multiple responses were permitted):

Table 5

Steps Taken To Prevent/Deter Computer Crime

Action	Number of respondents	Percentage of total (274)
Limited access to computer program, computer logic	233	85%
Limited access to computer operations	223	81
Frequent changing of access codes, user ID numbers	198	72
Limited access to input of data into computer	195	71
Installation of asset controls and accountability	157	57
Frequent security checks of computer and operations	137	50
Security education for employees	135	49
Improved screening of employees who have access to computers	114	42
Severe sanctions for employees involved in computer-related irregularities	101	37
Prompt referral of suspected illegal activity to law enforcement authorities	54	20
Coding of input data	39	14
Coding of output data	39	14
Other	34	12

(Total number of respondents = 274)

The respondents were next asked their views on the need for a federal criminal statute specifically directed to computer crime. Their responses were as follows:

Table 6

Views Regarding Need for
Federal Criminal Statute
Directed Specifically to Computer Crime

Position	Number of respondents	Percentage of total (280)
Strongly support such a statute	163	58%
Somewhat support such a statute	58	21
Have no opinion regarding the need for such a statute	43	15
Somewhat oppose such a statute	12	4
Strongly oppose such a statute	4	1
Total number of respondents	280	99%

The respondents were not asked to evaluate any specific proposed statutory language. The fact that 79% of them either strongly support or somewhat support the passage of some federal computer crime statute, however, appears noteworthy.

D. Most Troublesome Current and Future Aspects of Computer Crime

The survey respondents were asked to describe, in their own words, "the most troublesome aspect of computer crime, currently and in the foreseeable future." Over 60% (175) of the respondents chose to provide comments. While the respondents' comments often made several points and also required some interpretation, they fell roughly into the following major categories:

Table 7

Most Troublesome Current and Future Aspects of Computer Crime

Problem	Number of respondents	Percentage of total (175)
Proliferation of business and personal computers and computer users	40	23%
Difficulty detecting computer crime	36	21
Vulnerability, lack of adequate security measures	35	20
Lack of public and/or managerial awareness and concern	24	14
Increasing reliance on computers/ magnitude of potential losses	19	11
Difficulty of prosecution/lack of prosecutorial interest or measures	17	10
Lack of adequate statutes/criminal sanctions	16	9
Lack of understanding of problem/ law enforcement expertise	16	9
Lack of clear definition/failure to recognize as crime	13	7
Espionage and spying, foreign and domestic	8	5

(Total number of respondents = 175)

In our Report on Computer Crime, we included verbatim the comments of twenty-five respondents, selected both for their tone and their substance. The respondents' comments express, as well as anything we have seen, the breadth and the depth of concern that private organizations and public agencies share concerning computer crime. We are, therefore, prepared to release to the Subcommittee and its staff, the

contents of all the comments received by the Task Force. The anonymity of the survey respondents will be protected by providing only the comments themselves and the primary type of business of the respective respondents providing them. These comments are contained in an Appendix to this Statement.

II. SIGNIFICANCE OF SURVEY RESULTS AND RECENT DEVELOPMENTS

A. The Subcommittee's Report

Although this Subcommittee's April 1984 Report dealt with many issues beyond the scope of our Task Force survey and Report, the findings of our Report are consistent with and supportive of several of this Subcommittee's findings. For example, in your Report you found that (Subcommittee Report at 3):

> "There is a need for effective and low cost computer/communications safeguards. Countermeasures are sometimes deemed too costly and system managers are reluctant to invest in technologies which may hamper systems performance or limit systems use. Appropriate technological protective measures do not exist for all applications; therefore, there is a need to promote research and development of security technologies with lower cost and greater efficiency."

As we noted in our Report, the comments from the survey respondents repeatedly indicated a concern regarding the lack of effective computer security technology, as well as

a lack of sufficient management concern regarding computer security problems (ABA Report at 30-31, 43). The survey results indicate the existence of an apparent gap between computer technology generally and computer security technology specifically, and thus support the Subcommittee's finding.

Secondly, the Subcommittee Report found that while media attention focuses on the threat of "computer hackers" and other outside intruders, "the greatest threat to computerized resources remains personnel who are authorized to access them." (Subcommittee Report at 3.) The survey responses concerning the identity of perpetrators of known computer crime incidents, discussed above, support the Subcommittee's finding, although recent incidents of "computer hacking", discussed below, indicate that such activity by outsiders can have widespread and devastating results.

Thirdly, the Subcommittee Report found that (Subcommittee Report at 5):

> "There is a shortage of capable and well-trained computer security personnel ... The lack of trained criminal justice officials limits detection and successful prosecution of cases involving computer crime and abuse."

The responses to our survey indicated that both private industry and public officials believe that law enforcement personnel do not have the expertise necessary to investigate and prosecute computer crime successfully (ABA Report at

44-45). This response supports the Subcommittee's finding and also explains, in part, the high proportion of computer crime incidents that are not reported to law enforcement officials.

An incident reported in The Washington Post on September 9, 1984, illustrates well, I think, the disparity between the skills and expertise of computer criminals compared to those of many law enforcement officials. The news article, which is attached to my Statement, describes the arrest of a 13 year-old Columbia, Maryland youth, based on a tip from an informant, for allegedly using data supplied by computer pirates from around the country to make illegal credit card purchases, place free long-distance telephone calls and obtain hundreds of bootlegged computer programs worth as much as $20,000. The Howard County police seized the 13 year-old's computer, but none of them had any idea how it worked. The FBI provided technical assistance to the local police, but the only way the local investigators could fully grasp what the 13 year-old had done was to watch "in amazement" as he demonstrated wnat he had done and how easy it was to accomplish.

Finally, the Subcommittee Report notes that "[t]he lack of reliable statistics on computer/communications systems abuses contributes to a misunderstanding of the problem and hampers implementation of adequate safeguards."

(Subcommittee Report at 6.) The work of our Task Force indicates that the Subcommittee finding in this respect is correct. In both the private and public sectors, there is a remarkable lack of knowledge concerning the nature and extent of computer crime. Gathering and maintaining more meaningful and comprehensive data, however, will be no easy task.

B. The Need for Federal Computer Crime Legislation

In our Report, we noted that the American Bar Association first endorsed the adoption of federal computer crime legislation in 1979, acting on a resolution from the Criminal Justice Section. (ABA Report at 45.) The ABA's position in favor of federal computer crime legislation is fully supported by the results of our Task Force survey and by recent events.

Federal legislation is necessary and would be beneficial for a number of reasons:

1. The existence of a federal criminal statute specifically directed at computer-related illegal activity should dispel the perception, apparently shared by a significant portion of the population, that computer abuse is a "game" that one may engage in freely without fear of prosecution or concern for the damage that may result.

2. A federal computer crime statute should aid law enforcement efforts generally by providing investigators and prosecutors a specific jurisdictional hook and a framework for prosecution, by encouraging private citizens to report computer crime, and by increasing the likelihood that law enforcement personnel will receive additional computer crime training.

3. Federal computer crime legislation will make the sanctions for committing computer crime more rational and more consistent with the seriousness of the crime.

4. A federal computer crime statute will assist the federal government in protecting itself and the public at large against the potentially devastating effects of manipulation or destruction of the government's computers and computer systems, upon which we are becoming increasingly dependent.

5. The passage of a federal computer crime statute is also likely to enhance the collection of meaningful data concerning the occurrence and nature of computer crime and the outcomes of investigation and prosecution of such crime.

For these and other reasons, the American Bar Association strongly supports the passage of federal computer crime legislation. We do so fully aware of the fact that the passage of such legislation is only part, albeit an important part, of a comprehensive public and private effort to combat the serious problem of computer crime.

We have yet to take an official position on the merits or demerits of specific computer crime legislation now pending in the House or the Senate. Our Task Force is currently reviewing both pending federal legislation and existing state statutes concerning computer-related crime.

C. Recent Developments

Less than two weeks after our Report on Computer Crime was released, the unauthorized infiltration of computers

containing the Nation's largest credit reporting data bank was disclosed. The incident, involving the credit histories of 90 million people contained in the files of TRW Information Systems, is one of the largest, if not the largest, reported incident of computer crime, in terms of the potential number of people directly affected. Based on press reports,*/ the facts are as follows:

The TRW computerized credit files are accessible by retail stores and other subscribers by means of a password, which is given to subscribers. The password was improperly obtained by someone from a Sears, Roebuck & Company store on the West Coast. The password was then posted on an electronic bulletin board, which made it available to all of the bulletin board subscribers. Once the password was obtained, a computer user could use it, along with publicly available information such as a credit cardholder's name, address and date of birth, to obtain numbers of all credit cards owned by the cardholder, as well as other credit information. This information, in turn, could be used to charge merchandise to the cardholders' credit cards.

According to TRW, the password could have been illegally used anywhere from a week up to a month, before TRW

---

*/ News articles appearing on June 22, 1984, in Newsday, The New York Times and The Washington Post.

discovered the breach and changed the password. TRW reported that there was no "unusual activity" involving the use of the password during the relevant period, but there apparently is no way to determine who used the password improperly during the period, what information was improperly obtained from the data bank, and what use was made of that improperly obtained information. The extent of improper use may only be known if the 90 million credit cardholders in the data bank notice and report improper and unauthorized charges appearing on their credit card statements and, even then, tracing these charges back to the breach of TRW's computers may be impossible. Finally, it should be noted that TRW found out about the improper infiltration of its computers only because of a tip from an informant.

The TRW incident, regardless of the actual monetary losses that resulted from it (which we will probably never know), is significant in a number of respects. First, it demonstrates the potential magnitude of losses that can result from a single computer security breach. Beyond the economic losses that any of 90 million people may have suffered, improper access to financial information concerning these individuals raises major privacy concerns. Secondly, the TRW incident raises a number of legal questions concerning the responsibility of those who store, compile, transmit, or otherwise use data stored in computer memory. What are, or should be, the legal responsibilities of those who compile and maintain such

records, like TRW? What are, or should be, the legal responsibilities of those who provide or have access to such data, like Sears Roebuck? What are, or should be, the legal responsibilities of those who operate, and subscribe to, electronic bulletin boards?

Finally, and perhaps the most troubling aspect of the TRW incident, what if there had not been an informant? How long would the breach of the computer records have continued before it was detected? How many other similar incidents have occurred, or are now occurring, that we simply know nothing about? The recent Maryland case involving a 13 year-old that I mentioned previously was uncovered only because of an informant. The same was true for an incident, similar to the TRW situation, involving a computerized credit record file in Atlanta in 1983.

In sum, the TRW incident, the responses to our survey, and other available information all indicate the enormous exposure that private and public agencies now have to computer crime of different varieties, and how difficult it is to prevent such crime in the first place, to detect it once it has occurred, and to investigate and prosecute it, if and when it is detected.

III. CONCLUSION

In closing, Mr. Chairman, I would like to indicate our support for this Subcommittee's efforts to examine and come to grips with a problem that affects, and will continue to affect, millions of American citizens and private and public institutions. For our part, our Task Force and others in the American Bar Association intend to continue to study computer crime, to contribute to the public debate on the subject, and to recommend specific steps that need to be taken by the public and private sectors to minimize and prevent the occurrence of computer crime. We hope to publish a second report in the coming months which will describe more specifically the legislative and policy actions that should be taken in order to deal more effectively with a problem that deserves serious and more sustained attention.

I will be happy to respond to any questions that any of you may have.